
MANAGING HEALTH CARE INFORMATION SYSTEMS

A Practical Approach for
Health Care Executives

Karen A. Wager, Frances Wickham Lee,
John P. Glaser

Foreword by Lawton Robert Burns



MANAGING HEALTH CARE INFORMATION SYSTEMS

MANAGING HEALTH CARE INFORMATION SYSTEMS

A Practical Approach for
Health Care Executives

Karen A. Wager, Frances Wickham Lee,
John P. Glaser

Foreword by Lawton Robert Burns

Copyright © 2005 by John Wiley & Sons, Inc. All rights reserved.

Published by Jossey-Bass

A Wiley Imprint

989 Market Street, San Francisco, CA 94103-1741 www.josseybass.com

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-646-8600, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, 201-748-6011, fax 201-748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: While the publisher and the author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Excerpts from the *Journal of AHIMA* are adapted and reprinted with permission from the American Health Information Management Association. Copyright © 2004 by the American Health Information Management Association. All rights reserved. No part of this material may be reproduced, reprinted, stored in a retrieval system, or transmitted, in any form or by any means, electronic, photocopying, recording, or otherwise, without prior written permission of the association.

Some sections of Chapters Eleven through Fifteen originally appeared in J. Glaser, *The Strategic Application of Information Technology in Healthcare Organizations*, 2nd ed. (San Francisco: Jossey-Bass, 2002). This material is used with the permission of John Wiley & Sons, Inc.

In addition, some sections of Chapters Eleven through Fifteen originally appeared in the following articles published in *Healthcare Financial Management*: J. Glaser, "Analyzing Information Technology Value," March 2003, pp. 98–104; J. Glaser, "Why Does an IT Investment Fail to Deliver Returns?" April 2003, pp. 114–118; J. Glaser, "When IT Excellence Goes the Distance," September 2003, pp. 102–106; J. Glaser, "The Mystery of IT Strategy," January 2004, pp. 82–84; J. Glaser, "Using Vectors to Minimize the Mystery of IT Strategy Development," March 2004, pp. 94–98; J. Glaser, "Back to Basics: Managing IT Projects," July 2004, pp. 34–38; J. Glaser, "Management's Role in IT Project Failures: Part I," October 2004, pp. 90–92; J. Glaser, "Management's Role in IT Project Failures: Part II," forthcoming. These materials are used with the permission of the Healthcare Financial Management Association.

Jossey-Bass books and products are available through most bookstores. To contact Jossey-Bass directly call our Customer Care Department within the U.S. at 800-956-7739, outside the U.S. at 317-572-3986, or fax 317-572-4002.

Jossey-Bass also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data

Wager, Karen A.

Managing health care information systems : a practical approach for health care executives / by Karen A. Wager, Frances Wickham Lee, John P. Glaser. — 1st ed.

p. ; cm.

Includes bibliographical references and index.

ISBN-13 978-0-7879-7468-8 (alk. paper)

ISBN-10 0-7879-7468-4 (alk. paper)

1. Medical informatics. 2. Health services administration.

[DNLM: 1. Medical Informatics—organization & administration. W 26.5

W133m 2005] I. Lee, Frances Wickham, II. Glaser, John (John P.) III.

Title.

R858.W34 2005

362.1'068—dc22

2004026198

Printed in the United States of America

FIRST EDITION

HB Printing 10 9 8 7 6 5 4 3 2 1

CONTENTS

Tables, Figures, and Exhibits ix

Foreword xiii

Acknowledgments xv

About the Authors xvii

Introduction xix

PART ONE: HEALTH CARE INFORMATION 1

1 Introduction to Health Care Information 3

2 Health Care Data Quality 43

3 Health Care Information Regulations, Laws, and Standards 61

PART TWO: HEALTH CARE INFORMATION SYSTEMS 89

4 History and Evolution of Health Care Information Systems 91

5 Current and Emerging Use of Clinical Information Systems 111

- 6 System Acquisition 146
- 7 System Implementation and Support 167

PART THREE: INFORMATION TECHNOLOGY 187

- 8 Information Architecture and Technologies That Support Health Care Information Systems 189
- 9 Health Care Information System Standards 233
- 10 Security of Health Care Information Systems 250

PART FOUR: SENIOR MANAGEMENT IT CHALLENGES 279

- 11 Organizing Information Technology Services 281
- 12 IT Alignment and Strategic Planning 314
- 13 IT Governance and Management 361
- 14 Management's Role in Major IT Initiatives 390
- 15 Assessing and Achieving Value in Health Care Information Systems 418

Appendixes

- A Overview of the Health Care IT Industry 449
- B Sample Project Charter 461

References 473**Index 486**

TABLES, FIGURES, AND EXHIBITS

Tables

- 1.1 Examples of Types of Patient Encounter Data and Information
- 1.2 Federal Employees Health Benefits Program: HEDIS Quality Measures
- 2.1 AHIMA Data Quality Management Characteristics
- 2.2 Some Causes of Poor Health Care Data Quality
- 4.1 Common Types of Administrative and Clinical Information Systems
- 4.2 Timeline of Major Events + Advances in Information Technology = HCIS
- 5.1 Some Current Reimbursement Strategies
- 6.1 Sample Criteria for Evaluation of a Vendor's RFP Responses
- 8.1 Differences Between OLTP Databases and Data Warehouses
- 8.2 Seven-Layer OSI Model
- 9.1 Organizations Responsible for Formal Standards Development
- 10.1 An Insurer's Personal Loss Claims for Hardware in 2002
- 11.1 Managers' Grades for Work Factors
- 12.1 IT Support of Organization Goals
- 12.2 Summary of the Scope of Outpatient Care Problems
- 12.3 Potential Value Proposition for Wireless Technology
- 12.4 Sample Synthesis of IT Strategic Planning
- 13.1 Target Increases in an IT Operating Budget
- 14.1 Project Resource Analysis

- 15.1 Financial Analysis of a Patient Accounting Document Imaging System
- 15.2 Requests for New Information System Projects
- A.1 Typical Provider Distribution of IT Spending
- A.2 Health Care Vertical Market: NAICS Taxonomy
- A.3 Major Health Care IT Vendors: Ranked by Revenue

Figures

- 1.1 Types of Health Care Information Framework
- 1.2 Sample EMR Screen
- 1.3 Inpatient Encounter Flow
- 1.4 Physician's Office Visit Patient Flow
- 1.5 UHDDS Elements and Definitions
- 1.6 Excerpt from the ICD-9-CM Disease Index
- 1.7 Patient Encounter Form
- 1.8 Example of Diabetes Query Screen
- 1.9 Sources of Comparative Data for Health Care Managers
- 1.10 Two CMS Data Charts
- 1.11 Sample Electronic Knowledge-Based Information Resources
- 2.1 From Data to Knowledge
- 2.2 AHIMA Data Quality Management Model
- 2.3 Activities for Improving Data Quality
- 3.1 Medical Record Content: Excerpt from South Carolina Standards for Licensing Hospitals and Institutional General Infirmaries
- 3.2 Medical Record Content: Excerpt from the Conditions of Participation for Hospitals
- 3.3 JCAHO Overview of Management of Information
- 3.4 JCAHO Standards for the Content and Maintenance of Patient Records
- 3.5 AHIMA Guidelines for Defining the Health Record for Legal Purposes
- 3.6 Recent Health Care Privacy Violations
- 4.1 Typical Mainframe Computer
- 4.2 Physician Using a PDA
- 5.1 Five Levels of Computerization
- 5.2 Sample Drug Alert Screen
- 5.3 Sample EMR Screen
- 5.4 Profile of the 2003 Nicholas E. Davies Award Recipient: Primary Care Practice Category
- 5.5 Profile of the 2003 Nicholas E. Davies Award Recipient: Organizational Category

- 5.6 Sample CPOE Screen
- 5.7 Projected Benefits of Implementing Advanced Ambulatory CPOE Systems
- 5.8 Sample E-Mail Communication Policy
- 5.9 EMR: The Hub of Clinical Information Systems
- 6.1 Overview of System Acquisition Process
- 6.2 Sample Project Repository
- 6.3 Sample Gantt Chart
- 7.1 Sample Composition of Implementation Team
- 7.2 Components of Implementation Plan
- 8.1 Common Interface Engine Operation
- 8.2 Relational Database Management System Components
- 8.3 Entity Relationship Diagram
- 8.4 Partial Attribute Lists for *Patient*, *Clinic*, and *Visit*
- 8.5 Data Flow in the OSI Model
- 8.6 OSI Model Compared to the Internet Model
- 8.7 Bus and Ring Topologies
- 8.8 Physical Star Topology
- 8.9 Ethernet Network in a Physical Star
- 8.10 XML and HTML Code
- 8.11 URL Components
- 8.12 Touch Screen
- 8.13 Thumb Drive
- 8.14 Laptop Computer
- 8.15 Tablet Computer
- 8.16 Personal Digital Assistant
- 9.1 HL7 Encoded Message
- 9.2 HL7 EHR Functional Model Outline
- 9.3 Conceptual Model of the CCR
- 10.1 Outsider Breaches
- 10.2 Insider Breaches
- 10.3 Encryption Procedure
- 11.1 Typical IT Organization Chart
- 11.2 Sample CIO Job Description
- 11.3 Sample CMIO Job Description
- 11.4 IT Department Organized by Function and Geography
- 11.5 IT Department Organized by Function and Process
- 12.1 Vectors for Arriving at IT Strategy
- 12.2 IT Initiatives Necessary to Support a Strategic Goal for a Provider
- 12.3 IT Initiatives Necessary to Support a Strategic Goal for a Health Plan
- 12.4 System Support of Nursing Documentation

- 12.5 IT Initiative Priorities
- 12.6 Plan Timelines and Budget
- 12.7 Singles and Grand Slams
- 13.1 IT Budget Decision-Making Process
- 14.1 Project Timeline With Project Phases
- 14.2 Project Status Report
- 15.1 IT Investment Portfolio
- 15.2 Days in Accounts Receivable Before and After Implementation of Practice Management System

Exhibits

- 1.1 Uniform Bill: UB-92
- 1.2 Claim Form: CMS-1500
- 1.3 Section of a Medicare Cost Report for a Skilled Nursing Facility
- 1.4 HEDIS 2004 Summary Table of Measures and Product Lines
- 3.1 Sample Release of Information Form
- 11.1 Sample User Satisfaction Survey

FOREWORD

Information systems (IS) constitute the source of many of the problems in the health care industry. Health care is one of the most transaction-intensive industries (estimated at thirty billion transactions annually), given all the encounters between patients and providers, providers and other providers, providers and insurers, suppliers and providers, and so on. Yet compared to other industries, health care has historically underinvested in IS—and it shows. The transactions between parties in health care take place not so much electronically as through a mixture of telephone, paper, fax, and EDI media. The result is that much information is never captured, is captured incorrectly, is captured inefficiently, or is difficult to retrieve and use. Moreover, the industry relies heavily on legacy systems that cannot communicate with one another, not only between organizations but often within the same organization.

What is required to fix this messy situation? To paraphrase an old adage, the system may be the solution. The U.S. health care industry is in need of a massive infusion of capital to fund the adoption of new information technology (IT). Kaiser Permanente's plan to invest \$3.2 billion in a paperless system over ten years provides a glimpse of the scale involved. Who will offer providers (where much of the IS help is needed) the financial assistance to underwrite these investments? Providers will need support from their trading partners (for example, manufacturers who sell them products) and a big nudge from private sector insurers and (especially) the federal government in terms of how they pay for health care. Linking IT use to reimbursement is one step in the right direction. In addition, provider organizations will need to provide incentives to

their own physicians to employ IT—for example, by linking IT use to credentialing decisions. Finally, to convince all parties to adopt the necessary IT systems, we will need rigorous studies that document the cost and quality returns from these investments and the parties to which these returns accrue. This is not a small task.

This book provides an incredibly thorough overview of information systems and their importance in the health care industry. It provides an overview of the health care IT industry; a history of health care IS in the United States; a review of the fundamental characteristics of information, the uses to which it is put, and the processes it supports; and a highly detailed discussion of the primary clinical and managerial applications of information (including electronic medical records), the value of information and IS to multiple stakeholders, and most important, the management of information and IS. This approach is particularly helpful when one considers that the vast majority of health system executives underwent their graduate training at a time when information systems were in their infancy and thus when no such text existed. This volume is a great primer, offering a systematic presentation of a complex, important topic.

The reader will benefit from the collaborative effort that went into this volume. The first two authors are academics with considerable experience in teaching health care information management; the third is the chief information officer at one of the most prominent hospital (and integrated) systems in the United States. The combined talents of these two academics and one practitioner (all of whom have doctoral degrees) are reflected in the scope and depth presented here. This book is both systematic and practical, serving the needs of graduate students and current executives in the industry. What I have found particularly helpful is its ability to show how information and IS integrate with the other functions of the health care provider organization. The reader comes away from this book with a more profound understanding of how information serves as the lifeblood of the institution and as the real glue that can cement together professionals and departments within a health care organization and that can also tie the organization more closely to its upstream trading partners (manufacturers, wholesalers, and group purchasing organizations) and downstream trading partners (insurers and managed care organizations). At the end of the day, information and IS construct the real pathway to the utopia sought by providers during the past decade: integrated health care.

This book is required reading for all those who toil in the field of health care management—whether as managers, professionals, consultants, suppliers and customers, students, or scholars. The topic of IS in health care is simply too important, and until recently too often ignored, to be left to haphazard learning. I commend the authors for their great contribution to the field of health care management and information management.

March 2005

Lawton Robert Burns
The James Joo-Jin Kim Professor
The Wharton School

ACKNOWLEDGMENTS

We wish to thank Brian M. Jones and Kristofer Kitzke, MHA graduate students at the Medical University of South Carolina, for their assistance in preparing the final manuscript for this book.

To our students

ABOUT THE AUTHORS

Karen A. Wager is associate professor in the Department of Health Administration and Policy at the Medical University of South Carolina, where she teaches health information system courses to graduate students. She has over twenty years of professional and academic experience in the health information management field and has published numerous articles, case studies, and book chapters. She is a senior member of the Healthcare Information and Management Systems Society (HIMSS) and an active member of both the American Medical Informatics Association (AMIA) and the American Health Information Management Association (AHIMA). She is a past president of the South Carolina Health Information Management Association and the South Carolina chapter of HIMSS. She holds a DBA degree from the University of Sarasota. Her research interests relate to the organizational aspects of incorporating clinical information systems into the community practice environment.

Frances Wickham Lee is associate professor in the Department of Health Administration and Policy at the Medical University of South Carolina (MUSC) in Charleston. Prior to joining the MUSC faculty in 1991, she was a faculty member at Western Carolina University. Her academic career spans nearly thirty years. She currently teaches health information management and applied database management to graduate and undergraduate students. She has published a variety of articles on topics related to health information management and health information systems and has been a contributing author to several health information management books in

recent years. A registered health information administrator (RHIA) and a certified professional in healthcare information and management systems (CPHIMS), she is an active member in both AHIMA and HIMSS. She received her DBA degree from the University of Sarasota.

John P. Glaser is vice president and chief information officer at Partners Health-Care System, Inc., which has received several industry awards for its effective and innovative use of information technology. Previously, Glaser was vice president of information systems at Brigham and Women's Hospital, and before that he managed the health care information systems consulting practice at Arthur D. Little. The founding chairman of the College of Healthcare Information Management Executives (CHIME), he is also a past president of HIMSS and a former member of the board of AMIA. He is currently the president of the Foundation for eHealth Initiative board. A fellow of HIMSS, CHIME, and the American College of Medical Informatics, he is a recipient of the John Gall award for health care CIO of the year and of *CIO* magazine's 20/20 Vision award. CHIME has established a scholarship in his name. He has published over ninety articles and two books on the strategic application of information technology in health care. He holds a Ph.D. degree in health care information systems from the University of Minnesota.

INTRODUCTION

Having ready access to timely, complete, accurate, legible, and relevant information is critical to health care organizations, providers, and the patients they serve. Whether it is a nurse administering medication to a comatose patient, a physician advising a patient on the latest research findings for a specific cancer treatment, a billing clerk filing an electronic claim, a chief executive officer justifying to the board the need for building a new emergency department, or a health policy analyst reporting on the cost effectiveness of a new prevention program to the state's Medicaid program, each individual needs access to high-quality information with which to effectively perform his or her job. The need for quality information in health care has never been greater, particularly as this sector of our society strives to provide quality care, contain costs, and ensure adequate access. At the same time, the demand for information has increased, we have seen unprecedented advances in information technology—such advances have the potential to radically change how health care services are accessed and delivered in the future.

To not only survive but thrive in this new environment, health care executives must have the knowledge, skills, and abilities to effectively manage both clinical and administrative information within their organizations and across the health care sector. Within the next decade or two, the predominant model for maintaining health care information will shift from the current, primarily paper-based medical record system, in which information is often incomplete, illegible, or unavailable where and when it is needed, to a system in which the patient's clinical and administrative

information is integrated, complete, stored electronically, and available to the patient and authorized persons anywhere, anytime—regardless of the setting in which services are provided or the health insurance or coverage the patient carries. Providers involved in the patient’s care will have immediate access to electronic decision-support tools, the latest relevant research findings on a given topic, and patient-specific reminders and alerts. Moreover health care executives will be able to devise strategic initiatives that take advantage of access to real-time, relevant administrative and clinical information.

The Purpose and Organization of This Book

The purpose of this book is to prepare future health care executives with the knowledge and skills they need to manage information and information system technology effectively in this new environment. We wrote the book with the graduate student (or upper-level undergraduate student) enrolled in a health care management program in mind. Our definition of health care management is fairly broad and includes a range of academic programs from health administration, health information management, public health, and master of business administration (MBA) programs (with an emphasis in health) to nursing administration and physician executive educational programs.

The chapters in this book are organized into four major sections:

Part One: “Health Care Information” (Chapters One through Three)

Part Two: “Health Care Information Systems” (Chapters Four through Seven)

Part Three: “Information Technology” (Chapters Eight through Ten)

Part Four: “Senior Management IT Challenges” (Chapters Eleven through Fifteen)

Part One, “Health Care Information,” is designed to be a health information “primer” for future health care executives. Often health information system textbooks begin with technology chapters and are written with an assumption that the reader understands the basic clinical and administrative information and the processes that create and use this information within a health care organization. They jump into health information system or technology solutions without first examining the fundamental characteristics of the information and processes such systems are designed to support (Chapter One), data quality (Chapter Two), or the laws, regulations, and standards that govern the management of information (Chapter Three) in health care organizations. It has been our experience that many students aspiring to be health care executives do not have a clinical background and therefore have a limited understanding of

patient care processes and the information that is created and used during these processes. And even though they may be well versed in business management functions, such as accounting and financial management, they may lack adequate knowledge of the unique features of the patient care process. The three chapters we have included in Part One are designed to set the stage and provide the requisite background knowledge for the remainder of the book. Students with extensive clinical or health information management backgrounds may skim this section as a refresher.

Part Two, “Health Care Information Systems,” provides the reader with an understanding of how health care information systems evolved and the major clinical and administrative applications in use today (Chapter Four). Special attention is given to the emerging use of clinical information systems, with a focus on electronic medical record (EMR) systems. Chapter Five focuses on the value of EMR systems to the patient, the provider, the health care organization, and the health care community at large. Other major types of clinical information systems are also discussed. Included are two applications used to manage the patient care process within the health care organization (computerized provider order entry [CPOE] and medication administration) and applications used to deliver patient care services or to interact with patients at a distance (for example, telemedicine and telehealth). We selected these systems because they have an enormous potential to improve quality, decrease costs, and improve patient safety; some of them are being widely debated and are likely to be hot topics in the coming years.

The last two chapters in Part Two describe the process that a health care organization typically goes through in selecting (Chapter Six) and implementing (Chapter Seven) a health care information system. We focus on vendor-acquired systems and describe the pros and cons of contracting with an application service provider (ASP), because most health care organizations are not equipped to develop their own applications. Despite the best-made plans, things can and do go wrong when an organization is selecting or implementing a health care information system. Chapter Six concludes with a discussion of the issues that can arise during the system acquisition process and strategies for addressing them. We devote a substantial section of Chapter Seven to the organizational and cultural aspects of incorporating information technology (IT) systems into the health care organization. Chapter Seven ends with a discussion of issues that can arise during system implementation and strategies for addressing them.

Part Two focuses on health care information systems and the value they can bring to health care organizations, providers, and the patients they serve. Part Three, “Information Technology,” turns to the technology underlying these systems, that is, how they work. The chapters in Part Three are designed to provide a basic understanding of information technology concepts such as architectures and the core technologies needed to support health care information systems in terms of databases (Chapter Eight),

networks (Chapter Eight), standards (Chapter Nine), and security (Chapter Ten). The intent is to provide the reader with enough IT knowledge that he or she could carry on a fairly intelligent conversation with a chief information officer (CIO) or a technically savvy clinician, understand the significance of having a sound technical infrastructure to support systems, and appreciate the significance of system security.

Part Four, “Senior Management IT Challenges,” provides a top-level view of what it takes to effectively manage, budget, govern, and evaluate information technology services in a health care organization. Chapter Eleven introduces the reader to the IT function, the services typically found in an IT department in a large health care organization, and the types of professionals and staff generally employed there.

We believe that it is critical for health care executives to become actively involved in discussions and decisions regarding their organization’s use of IT. These discussions are diverse, covering topics such as the organization’s IT strategy (Chapter Twelve), IT budgeting and governance (Chapter Thirteen), management’s role in major IT initiatives (Chapter Fourteen), and methods for evaluating return on investment or the value of health care information systems to the organization, the provider, and the patient (Chapter Fifteen). Part Four addresses these and other important management issues and suggests approaches for addressing them.

Each chapter in the book begins with an overview and concludes with a summary of the material presented. *Learning activities* are provided at the end of each chapter. These activities are designed to give the student an opportunity to explore more fully the concepts introduced in the chapter and to gain hands-on experience by visiting and talking with IT professionals in a variety of health care settings.

Two appendixes offer supplemental information. Appendix A presents an overview of the health care IT industry, the companies that provide IT hardware, software, and a wide range of services to health care organizations. Appendix B contains an example of a project charter.

Challenges to Effective Use of IT in Health Care

The health care industry is one of the most information intensive and technologically advanced in our society. Yet if you asked a roomful of health care executives and providers from a typical health care organization if they have easy access to timely, complete, accurate, reliable, and relevant information in making important strategic or patient-care decisions, most would respond with a resounding no. Despite the need for administrative and clinical information to facilitate the delivery of high-quality, cost-effective services, most organizations still function using paper-based or otherwise

insufficient information systems. There are many reasons why this situation exists, not the least of which is that the health care industry is complex, both overall and in many of its functions. This complexity poses challenges for both the purchasers and vendors of health care information systems and the related IT products and services.

Health care is often accused of being “behind” other industries in applying IT. Statistics, such as percentage of revenue spent on IT, are often used to indict health care for underinvesting in IT. If you look across all industries, the average proportion of revenue spent on IT is 3.9 percent, compared to health care where the proportion is about 2.5 percent (Cruz, 2003). The indictment of being behind often carries with it an aspersion that health care executives are not as sharp or “on top of it” as executives in other industries. This is not true.

The complexity of health care makes it very challenging to implement health care information systems and IT effectively. We emphasize this fact of complexity not to excuse health care organizations from having to make thoughtful investments nor to claim that all health care executives are world class but to make it clear that health care executives need to understand the complexity.

Large Numbers of Small Organizations

Health care has large numbers of very small organizations. A majority of physicians practice in one- to two-physician offices. Thousands of hospitals have fewer than 100 beds. There are over 7,000 home health agencies. The small size of these organizations means that it is difficult for them to fund information system investments. An investment of \$25,000 in an electronic medical record may be more than a solo practitioner can bear. These organizations rarely have IT-trained staff members and hence are challenged when technology misbehaves—for example, when a printer malfunctions or files are inadvertently deleted.

The small size of these organizations also makes it difficult for software and hardware vendors to make money from them. Often these vendors cannot charge much for their applications, making it difficult for them to recover the costs of selling to small organizations and providing support to them. As a result, major vendors often avoid small organizations. Those vendors that do sell to this market are often small themselves, having perhaps four to six customers. This smallness means that if they have even one bad year—for example, the loss of two customers—it may put them out of business. Hence there is significant turnover among small IT vendors. This turnover clearly places the small provider organization at risk of having the vendor of its IT system go out of business.

Unfortunately, there is no obvious answer to the IT challenges posed by the large numbers of small organizations in health care.

Incentive Misalignment

Many health care information system applications have the potential to improve the quality of care. CPOE can reduce adverse drug events. Reminder systems in the electronic medical record can improve the management of the chronically ill patient. These are worthy goals, and providers may opt to bear the costs of the systems to gain improved care. In truth, however, the provider does not always reap a reward for such actions. The insurance payment mechanism may not provide a fiscal reward for the provider who has fewer medical errors. There may be no direct fiscal reward for better management of the diabetic.

Because of this misalignment that means the bearer of the cost sees no fiscal reward, providers can, rightfully, be hesitant to invest in IT that has care quality improvement as its goal. For them the IT investment reduces their income—there is little upside. This misalignment rarely occurs in other industries. For example, if you are in the banking industry and your IT investments are intended to improve the quality of your service, you expect to be rewarded by having more customers and by having existing customers do more business with you.

Currently, several payers are experimenting with providing fiscal rewards for quality of care. In some of these experiments, providers are being given extra money when they use clinical systems. If these experiments do not lead to payment for quality mechanisms or if the payment is too small, the problem of incentive misalignment will continue. And the rate of adoption of IT by providers will remain slow.

Fragmented Care

Most of us, over the course of our lives, will seek care in several health care organizations. At times this care will also occur in various regions of the country. The data about our care are not routinely shared across the organizations we use. And the organizations do not have to be on different sides of this country for this failure to occur; they may be across the street from each other. This failure to share data means that any given provider may not be fully aware of allergies, history, and clinical findings that were recorded in other settings. Medical errors and inefficiencies, for example, unnecessary repeats of tests, can result.

To a large degree, medical information exchange has been hindered by the lack of standards for health care data and transactions. However, this problem is being resolved. The lack of exchange nevertheless continues. Although this is due in part to the fact that many providers still use paper-based systems that make exchange more expensive and less likely to happen, it occurs primarily because there is no incentive for either the sender or the receiver to make the exchange happen. It may seem odd, perhaps counter to the mission of health care, that organizations need fiscal

incentives to do what is best for the patient. However, it is a harsh reality of health care that organizations do need fiscal incentives.

Integrated delivery systems have been formed that attempt to reduce fragmentation. These systems attempt to pull together diverse types of health care organizations and use information systems to integrate data from these organizations. These efforts do ease fragmentation, but they do not entirely solve the problem. There are insufficient numbers of integrated delivery systems, wide variations exist in the degree to which they try to integrate care, and patients will often seek care outside the integrated delivery system.

The fact that patients seek care outside of the integrated delivery system poses significant challenges for these systems. These challenges are also present for an individual hospital. If an organization desires to create a composite clinical picture of a person—through the implementation of a clinical data repository, for example—it faces two fundamental problems (in addition to the lack of incentives and limited data and process standards):

- The organization may need clinical data from multiple care settings, potentially dozens or hundreds of settings. The resulting “pattern” of system interconnections, when existing over a region or a state and involving multiple provider organizations, is a complex network topology model, with almost every provider connected to every other provider. It may not be possible to make this model work.
- The desired data are randomly dispersed. The site where the patient is currently receiving care may not know whether other data about this patient exist or whether these other data are relevant. When a patient presents at the emergency room, care providers may not know whether the patient has been seen in other hospitals in the city.

Complexity of the Process of Care

If one views the process of care as a manufacturing process (sick people are inputs, a “bunch of stuff” is done to them, and better or well people emerge), it is arguable that medical care is the most complex manufacturing process that exists. This type of complexity has three major sources: the difficulty of defining the *best* care, care process variability, and process volatility.

Our current ability to define the best care process for treating a particular disease or problem can be limited. Process algorithms, guidelines, or pathways are often

- Based on heuristics (or rules of thumb), which makes consensus within and between organizations difficult or impossible. Available facts and science are often insufficient to define a consistent, let alone the most effective, approach. As a result, competing guidelines or protocols are being issued by payers, provider organization committees, and provider associations.

- Condition or context specific. The treatment of a particular acute illness, for example, can depend on the severity of the illness and the age and general health of the patient.
- Reliant upon outcome measurements that can have severe limitations. For example, they may be insensitive to specific interventions, be proxies for “real” outcomes, or reflect the bias of an organization or researcher.

An organization is unlikely to define or adopt a consistent approach for each type of care. And even a defined approach may permit substantial latitude on the part of the provider. In these cases, great variability in treatment can occur. In an academic medical center a physician may have at his or her disposal 2,500 medications (each with a set of “allowable” frequencies, doses, and routes), 1,100 clinical laboratory tests, 300 radiology procedures, and large numbers of other tests and procedures. The application sequence and time relationship of the items chosen from these sets, along with patient condition and comorbidity, all come together to determine the relative utility of a particular approach to treatment. The variability of approaches to treating a disease is compounded by the diversity of diseases and problems. There are 10,000 diseases, syndromes, and problems, each of which, in theory, has its own pathway, guideline, or approach and perhaps multiple approaches.

This variability, or opportunity for variability, is unparalleled by any other manufacturing process. No automobile manufacturer produces 10,000 different models of cars or provides for each model 2,500 different types of paint, 300 different arrangements of wheels, and 1,100 different locations for the driver’s seat.

If, through hard work and a very agreeable group of providers, we were finally able to develop a large number of guidelines and algorithms and to significantly reduce the options in test, medication, and procedure ordering, we would still be confronted with the volatility of the medical process. In an average year, 460,000 articles are added to the base of refereed medical literature, articles that may require us to continually revisit our consensus. In addition, medical technology often induces changes in practices before the studies that measure practice efficacy can be completed.

The complexity of the medical process places unique and tough demands on the design of clinical information systems, our ability to support provider and patient decision making, and our ability to measure the quality of the care that we deliver. It is a complex undertaking to rationalize or standardize these processes within one provider organization. Clearly, we compound the problem as we move across organizations within a system of care and, from there, expand beyond the boundaries of an integrated delivery system. We may be faced with the need to bring interoperability to application systems that support different approaches to care.

Complexity of Health and Medical Data

The health status and medical condition of a patient is difficult to describe using comprehensive, coded data. Several factors contribute to this problem:

- Although research is ongoing, well-accepted methods to formally decompose many key components of the patient record, for example, admission history and physical status, into coded concepts have not yet been developed.
- Even when such data models have been developed, vocabularies to represent the terms within the model in a standard way are difficult to develop. The condition of a patient is often complex and probabilistic, requiring a nuanced description. Multifactorial and temporal relationships can exist between pieces of data. This complexity makes it inherently difficult to develop codes for medical data.
- Even when the data model has been developed and coded terms defined, the entry of coded data is cumbersome and constraining for the provider compared to using ordinary text.
- Finally, no single way exists to organize automated medical data; the relational model does not serve the medical domain particularly well; and many idiosyncratic ways to code data, across sites and often within a single site, have been developed. The latter have often been devised for good reasons, and because of the significant investments made to define and implement these idiosyncratic methods, change will not happen unless the need for it is very compelling.

Because coding schemes can be idiosyncratic, nonexistent, or insufficient within and across organizations, establishing clinical meaning, measuring care, determining the health status of a patient, and developing clinical information systems that interoperate can be exquisitely difficult.

The Nature of Provider Health Care Organizations

Health care organizations, particularly providers, have attributes that can hinder information system adoption. Provider organizations are unusual in that they have two parallel power structures: administration and the medical staff. The medical staff side is often loosely organized and lacks an organization chart with clear lines of authority. This two-part structure leads to a great deal of negotiating and coalition building. Negotiation is an aspect of any major decision within a provider organization, including decisions about health care information systems. This can result in very long decision-making cycles; reaching an agreement on an IT vendor can take months or years. At times agreement cannot be reached, and the organization fails in its efforts to advance in its use of IT.

Rising to the Challenge

We do not intend this discussion of complexity to lead the reader to the edge of inconsolable despair, only to an understanding of the landscape. Despite the complexity described here, significant progress may be made. Health care is carried out by many small organizations, but advances are being made in developing inexpensive, very robust IT applications. Efforts are under way to address the problem of misaligned incentives. The care process is complex, but the appropriate way to manage diabetes (and many other diseases) is well understood. Medical data are complex, but there are established data standards for diseases, procedures, and laboratory tests. Care crosses boundaries, but an electronic medical record that has most of a patient's data is better than a paper record that has most of a patient's data.

Both the consumers and suppliers of health care information system products and services struggle to develop and implement systems that improve care and organizational performance. And their efforts are often successful. These efforts confront the health care industry's core challenges—size, fragmentation, misaligned incentives, and the complexity of care processes and medical data.

Health care consumers, payers, and purchasers are demanding that more be done to ensure that health care providers are equipped with the information needed to decrease administrative costs, improve access to care, and improve patient safety, in spite of the significant industry challenges. We hope you will find this book to be a useful resource in ensuring that your health care organization and its information systems are well equipped to handle patients', providers', administrators', and all other stakeholders' health care information needs.

MANAGING HEALTH CARE INFORMATION SYSTEMS



PART ONE

HEALTH CARE INFORMATION



CHAPTER ONE

INTRODUCTION TO HEALTH CARE INFORMATION

Although it may seem self-evident, it is worth stating: *health care information is the reason we need health care information systems*. No study of information systems in health care would be complete without an examination of the data and information they are designed to support. The focus of this chapter will be on the data and information that are unique to health care, such as the clinical information created during patients' health care encounters, the administrative information related to those encounters, and the external information used to improve the clinical care and administrative functions associated with those encounters.

We begin the chapter with a brief discussion of some common definitions of health care information. Then we introduce the framework that will be used for exploring various types of health care information. The first section of the chapter looks at data and information created internally by health care organizations, discussing this information at both the individual level and the aggregate level. This chapter also examines some core processes involved in an inpatient and an ambulatory care clinical encounter to further explain how and when internal health care data and information originates and how it is used. The final section of this chapter examines health care data and information created, at least in part, externally to the health care organization, and addresses both comparative and knowledge-based data and information.

Types of Health Care Information

Different texts and articles define health care information or health information differently. Often it is the use or setting of the health information that drives the definition. For example, the government or an insurance company may have certain definitions of health care information and the hospital, nursing home, or physicians' offices others. In this book we are primarily interested in the information *generated or used by health care organizations*, such as hospitals, nursing homes, physicians' offices, and other ambulatory care settings. Of course this same information may be used by governmental agencies or insurance companies as well.

HIPAA and JCAHO Definitions

The Health Insurance Portability and Accountability Act (HIPAA), the recent, sweeping federal legislation that includes provisions to protect patients' health information from unauthorized disclosure, defines *health information* as "verbal or written information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse that relates to the physical or mental health of an individual, or payment for provision of health-care." HIPAA specifically refers to this type of information as "protected health information," or PHI. To meet the definition of PHI, information must first of all be "identifiable," that is, the information has an individual patient perspective and the patient's identity is known. HIPAA-defined PHI may exist outside a traditional health care institution and is therefore not an appropriate definition for an organizational view of information such as ours. HIPAA is certainly an important piece of legislation, and it has a direct impact on how health care organizations create and maintain health information (HIPAA is discussed further in Chapter Three). However, not *all* the information that must be managed in a health care organization is protected health information. Much of the information used by health care providers and executives is neither patient specific nor identifiable.

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO), the major accrediting agency for health care organizations in the United States, offers a framework for examining health care information within health care organizations. JCAHO accreditation standards have been developed over the years to, among other things, measure the quality of the different types of health care information that are found in and used with health care organizations. JCAHO (2004a) urges health care leaders to take "responsibility for managing information, just as they do for . . . human, material, and financial resources." JCAHO clearly acknowledges the vital role that information plays in ensuring the provision of quality health care.

JCAHO (2004a) divides health care information into four categories:

- Patient-specific data and information
- Aggregate data and information
- Knowledge-based information
- Comparative data and information

Although the JCAHO framework is for information at the organizational level, it is a little too general for our purposes. Therefore we have outlined a framework for this book that expands on JCAHO’s basic division of health care information.

Framework for Discussing Types of Health Care Data

Our framework for looking at data and information created, maintained, manipulated, stored, and used within health care organizations is shown in Figure 1.1. The first level of categorization in our framework is *internal* versus *external*.

Within the broad category of data and information created *internally* by the health care organization, we will focus on clinical and administrative information directly related to the activities surrounding the *patient encounter*, both individual encounters and collective encounters. We break information related to the patient encounter into the subcategories of *patient specific*, *aggregate*, and *comparative*. Our focus is on the clinical and administrative individual and aggregate health care information that is associated with a patient encounter. Table 1.1 lists the various types of data and information that fall into the patient encounter subcategories of patient-specific and aggregate. Information

FIGURE 1.1. TYPES OF HEALTH CARE INFORMATION FRAMEWORK.

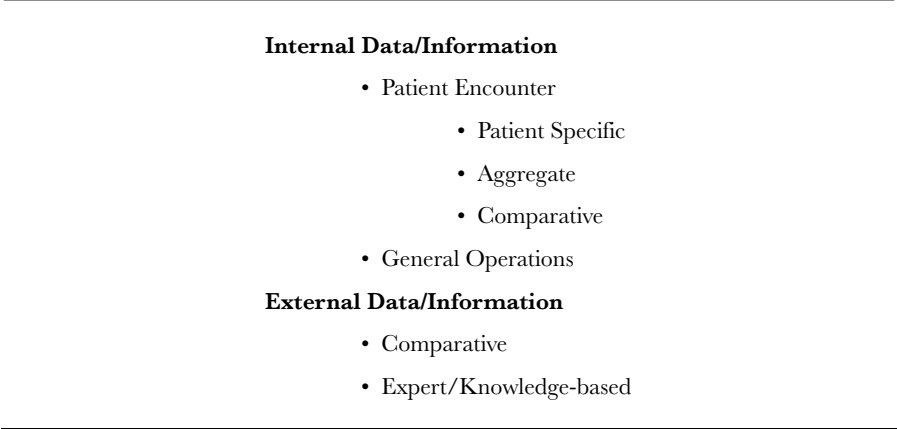


TABLE 1.1. EXAMPLES OF TYPES OF PATIENT ENCOUNTER DATA AND INFORMATION.

Type	Primary Purpose	
	Clinical	Administrative
Patient-specific (<i>items generally included in the patient medical record are in italics</i>)	<i>Identification sheet</i> <i>Problem list</i> <i>Medication record</i> <i>History</i> <i>Physical</i> <i>Progress notes</i> <i>Consultations</i> <i>Physicians' orders</i> <i>Imaging and X-ray results</i> <i>Lab results</i> <i>Immunization record</i> <i>Operative report</i> <i>Pathology report</i> <i>Discharge summary</i> Diagnoses codes Procedure codes	<i>Identification sheet</i> <i>Consents</i> <i>Authorizations</i> Preauthorization Scheduling Admission or registration Insurance eligibility Billing Diagnoses codes Procedure codes
Aggregate	Disease indexes Specialized registers Outcomes data Statistical reports Trend analysis Ad hoc reports	Cost reports Claims denial analysis Staffing analysis Referral analysis Statistical reports Trend analysis Ad hoc reports

typically found in a patient medical record is shown in italics. Although the comparative data and information subcategory is shown as part of both the internal and external categories, it will be discussed as part of the external data and information.

The second major component of internal health care information in our framework is *general operations*. Data and information needed for the health care organization's general operations are not a focus of this text. Health care executives do, however, need to be concerned not only with the information directly related to the patient encounter but also with information about the organization's general operations. Health care organizations are, after all, businesses that must have revenues exceeding costs to remain viable. The standard administrative activities of any viable organization also take place in health care settings. Health care executives interact with information and information systems in such areas as general accounting, financial planning, personnel administration, and facility planning on a regular if not daily basis. Our decision to focus on the information that is unique to health care and not a part of general business

operations is not intended to diminish the importance of general operations but rather is an acknowledgment that a wealth of resources for general business information and information systems already exists.

In addition to using internally generated patient encounter and general operations data and information, health care organizations use information generated *externally* (Figure 1.1). *Comparative* data, as we will explain, combine internal and external data to aid organizations in evaluating their performance. The other major category of external information used in health care organizations is *expert or knowledge-based* information, which is generally collected or created by experts who are not part of the organization. Health care providers and executives use this type of information in decision making, both clinical and administrative. A classic example of knowledge-based clinical information is the information contained in a professional health care journal. Other examples are regional or national databases or informational Web sites related to health or management issues.

Internal Data and Information: Patient Specific—Clinical

The majority of clinical, patient-specific information created and used in health care organizations can be found in or has as its original source patients' medical records. This section will introduce some basic components of a patient medical record. It will also examine an inpatient and an ambulatory care patient encounter to show how the patient medical record is typically created. All types of health care organizations—inpatient, outpatient, long-term care, and so forth—have patient medical records. These records may be in electronic or paper format, but the purpose and basic content are similar regardless of type of record or type of organization.

Purpose of Patient Records

There are several key purposes for maintaining medical records. As we move into the discussion of clinical information systems in subsequent chapters, it will be important to remember the reasons health care organizations keep medical records. These reasons remain constant whether the record is part of a state-of-the-art electronic system or part of a basic, paper-based manual system.

1. *Patient care.* Patient records provide the documented basis for planning patient care and treatment. This purpose is considered the *number one reason* for maintaining patient records. Health care executives need to keep this primary purpose in mind when examining health care information systems. Too often other purposes, particularly billing and reimbursement, may seem to take precedence over patient care.

2. *Communication.* Patient records are an important means by which physicians, nurses, and others can communicate with one another about patient needs. The members of the health care team generally interact with patients at different times during the day, week, or even month. The patient record may be the only means of communication between various providers.
3. *Legal documentation.* Patient records, because they describe and document care and treatment, can also become legal records. In the event of a lawsuit or other legal action involving patient care, the record becomes the primary evidence for what actually took place during the episode of care. An old but *absolutely true* adage about the legal importance of patient records says, “If it was not documented, it was not done.”
4. *Billing and reimbursement.* Patient records provide the documentation patients and payers use to verify billed services. Insurance companies and other third-party payers insist on clear documentation to support any claims submitted. The federal programs Medicare and Medicaid have oversight and review processes in place that use patient records to confirm the accuracy of claims filed. Filing a claim for a service that is not clearly documented in the patient record could be construed as fraud.
5. *Research and quality management.* Patient records are used in many facilities for research purposes and for monitoring the quality of care provided. Patient records can serve as source documents from which information about certain diseases or procedures can be taken, for example. Although research is most prevalent in large academic medical centers, studies are conducted in other types of health care organizations as well.

The importance of maintaining complete and accurate patient records cannot be underestimated. Not only do they serve as a basis for planning patient care, they also serve as the legal record documenting the care that was provided to patients by the organization. Patient medical records provide much of the source data for health care information that is generated within and across health care organizations. The data captured as a part of the patient medical record become a permanent record of that patient’s diagnoses, treatment, and response to treatment.

Content of Patient Records

The American Health Information Management Association sponsors the Web site www.myPHR.com, which lists the following components as being common to most patient records, regardless of the type of facility or whether the medical record system is electronic or paper based (myPHR, 2004). The specific content of medical records is determined to a large extent by external requirements, standards, and regulations (discussed in Chapter Three). This is not an exhaustive list, but it provides a

general overview of content and of the person or persons responsible for the content. It reveals that the patient record is a repository for varied clinical data and information that is produced by many different individuals involved in the care of the patient.

- *Identification sheet.* Information found on the identification sheet (sometimes called a *face sheet* or *admission/discharge record*) originates at the time of registration or admission. The identification sheet is generally the first report or screen a user will encounter when accessing a patient record. It lists at least the patient name, address, telephone number, insurance, and policy number, as well as the patient's diagnoses and disposition at discharge. These diagnoses are recorded by the physicians and coded by administrative personnel. (Diagnosis coding is discussed later in this chapter.) The identification sheet is used as both a clinical and an administrative document. It provides a quick view of the diagnoses that required care during the encounter. The codes and other demographic information are used for reimbursement and planning purposes.
- *Problem list.* Patient records frequently contain a comprehensive problem list, which lists significant illnesses and operations the patient has experienced. This list is generally maintained over time. It is not specific to a single episode of care and can be maintained by the attending or primary care physician or collectively by all the health care providers involved in the patient's care.
- *Medication record.* Sometimes called a *medication administration record* (MAR), this record lists medicines prescribed for and subsequently administered to the patient. This record often also lists any medication allergies the patient may have. Nursing personnel are generally responsible for documenting and maintaining medication information. In an inpatient setting, nurses are responsible for administering medications according to physicians' written or verbal orders.
- *History and physical.* The history describes any major illnesses and surgeries the patient has had, any significant family history of disease, patient health habits, and current medications. The information for the history is provided by the patient (or someone acting on his or her behalf) and is documented by the attending physician at the beginning of or immediately prior to an encounter or treatment episode. The physical component of the record states what the physician found when he or she performed a hands-on examination of the patient. The history and physical together document the initial assessment of the patient and provide the basis for diagnosis and subsequent treatment of the patient. They also provide a framework within which physicians and other care providers can document significant findings. Although obtaining the initial history and physical is a one-time activity during an episode of care, continued reassessment and documentation of that reassessment during the patient's course of treatment is critical. Results of reassessments are generally recorded in progress notes.

- *Progress notes.* Progress notes are made by the physicians, nurses, therapists, social workers, and other clinical staff caring for the patient. Each provider is responsible for the content of his or her notes. Progress notes should reflect the patient's response to treatment along with the provider's observations and plans for continued treatment. There are many forms of progress notes. In some organizations all care providers use the same note format, in others each provider type uses a specialized format.
- *Consultation.* A consultation note or report records opinions about the patient's condition made by physicians or other health care providers other than the attending physician or primary care provider. Consultation reports may come from people inside or outside a particular health care organization, but copies are maintained as part of the patient record.
- *Physician's orders.* Physician's orders are a physician's directions, instructions, or prescriptions given to other members of the health care team regarding the patient's medications, tests, diets, treatments, and so forth. In the current U.S. health care system, procedures and treatments must be ordered by the appropriate licensed practitioner; in most cases this will be a physician.
- *Imaging and X-ray reports.* The radiologist is responsible for interpreting images such as X-rays, mammograms, ultrasounds, scans, and the like and documenting his or her interpretations or findings in the patient's medical record. These findings should be documented in a timely manner so they are available to the appropriate physician(s) to facilitate the appropriate treatment. The actual films or images are generally maintained in the radiology or imaging departments as hard copies or in a specialized computer system. These images are typically not considered a part of the patient medical record, but they too are stored according to state laws and clinical practice guidelines, and they are an important documentation of patient care.
- *Laboratory reports.* Laboratory reports contain the results of tests conducted on body fluids, cells, and tissue. For example, a medical lab might perform a throat culture, urinalysis, cholesterol level, or complete blood count. There are hundreds of specific lab tests that can be run by health care organizations or specialized labs. Lab personnel are responsible for documenting the lab results. Results of the lab work become a part of the permanent patient record. However, lab results must also be available during treatment. Health care providers rely on accurate lab results in making clinical decisions, so there is a need for timely reporting of lab results and a system for ensuring that the physician(s) (or other appropriate care provider) receives the results. Physicians are responsible for documenting any findings and treatment plans that are based on the lab results.
- *Consent and authorization forms.* Copies of consents to admission, treatment, surgery, and release of information are an important component of the medical record related to its use as a legal document. The practitioner who actually provides the treatment must obtain the informed consent for the treatment. Patients must sign informed consent documents before treatment takes place. Forms authorizing release

of information must also be signed by patients before any patient-specific health care information is released to parties not directly involved in the care of the patient.

- *Operative report.* Operative reports describe any surgery performed and list the names of surgeons and assistants. The surgeon is responsible for the operative report.
- *Pathology report.* Pathology reports describe tissue removed during any surgical procedure and the diagnosis based on examination of that tissue. The pathologist is responsible for the pathology report.
- *Discharge summary.* Each hospital medical record contains a discharge summary. The discharge summary summarizes the hospital stay, including the reason for admission, significant findings from tests, procedures performed, therapies provided, response to treatment, condition at discharge, and instructions for medications, activity, diet, and follow-up care. The attending physician is responsible for documenting the discharge summary at the conclusion of the patient's stay in the hospital.

Figure 1.2 displays a screen from an electronic medical record. A patient record may contain some or all of the documentation just listed. Depending on the patient's illness or injury and the type of treatment facility, he or she may need specialized health care services. These services may require specific documentation. For example, long-term care facilities and behavioral health facilities have special documentation requirements. Our list is intended to introduce the common components of patient records, not to

FIGURE 1.2. SAMPLE EMR SCREEN.

Source: Partners HealthCare System, Inc.

provide a comprehensive list of all possible patient record components. As stated before, the patient record components listed here will exist whether the health care organization uses electronic records, paper records, or a combination of both.

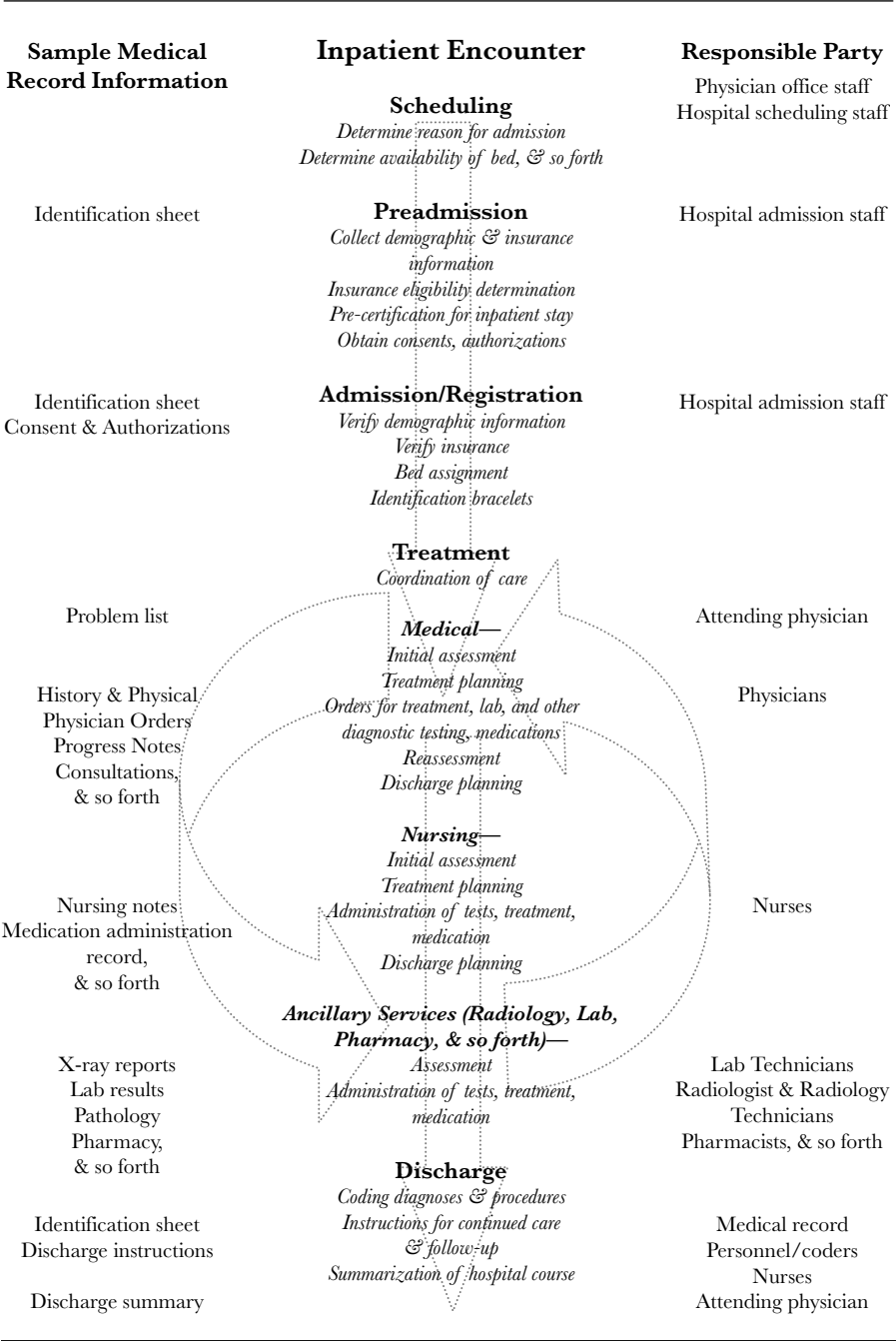
Overview of a Patient Encounter

Where do the medical record data and information come from? How do they originate? In this section we will walk through an inpatient encounter and also take a brief look at a physician's office patient encounter. Along the way we will point out how medical record information is created and used. Figure 1.3 diagrams a reasonably typical nonsurgical inpatient admission. The middle column represents the basic patient flow in an inpatient episode of care. It shows some of the core activities and processes the patient will undergo during a hospital stay. The left-hand column lists some of the points along the patient flow process where basic medical record information is added to the medical record database or file. The right-hand column lists the hospital personnel who are generally responsible for a patient flow activity or specific medical record documentation, or both. Using Figure 1.3 as a guide we will follow a patient, Mr. Marcus Low, through his admission to the hospital for radiation treatments.

Mr. Marcus Low's Admission. Mr. Low's admission to the hospital is scheduled by his oncologist, Dr. Good, who serves as the admitting and attending physician during Mr. Low's two-day hospital stay. Scheduling the admission involves the administrative staff in Dr. Good's office calling the Admissions Department of the hospital and arranging a time for Mr. Low to be admitted. The preadmission process involves the hospital corresponding or talking with Mr. Low and with Dr. Good's office to gather the demographic and insurance information that will be needed to file a claim with Mr. Low's insurance company. Generally, hospital personnel contact the patient's insurance company to precertify his or her hospital admission. In this case, in other words, the hospital checks that the insurance company agrees that Mr. Low's planned admission is medically necessary and will be approved for payment. The patient medical record is started during the preadmission phase. The Admissions Department must check whether Mr. Low has had a previous stay at the hospital and whether he has an existing medical record number or unique identifier. The *identification sheet* is started at this stage. Mr. Low's hospital has an electronic medical record system, so the demographic information needed is input into the computer system.

On the scheduled day of admission, Mr. Low arrives at the hospital's Admissions Department. There he verifies his demographic and insurance information. He is issued an identification (ID) bracelet and escorted to his assigned room by the hospital staff. Bed assignment is an important activity for the Admissions Department. It involves a great deal of coordination among the Admissions Department, nursing staff, and housekeeping

FIGURE 1.3. INPATIENT ENCOUNTER FLOW.



staff. Efficient patient flow within a hospital relies on this first step of bed assignment. Clean rooms with adequate staff need to be available not only for elective admissions like Mr. Low's but also for emergency admissions. Because the hospital has an electronic medical record, there is no paper chart to go to the nursing floor with Mr. Low, but the admissions staff verify that all pertinent information is recorded in the system. The admissions staff also have Mr. Low sign a general *consent to treatment* and the *authorization* that allows the hospital to share his health information with the insurance company.

Once on the nursing floor, Mr. Low receives a nursing assessment and a visit from the attending physician. The nursing assessment results in a nursing care plan for Mr. Low while he is in the hospital. Because Mr. Low saw Dr. Good in his office during the previous week, the *history and physical* is already stored in the electronic medical record system. Dr. Good records his *orders* in the physician order entry component of the electronic medical record. The nursing staff responds to these orders by giving Mr. Low a mild sedative. The Radiology Department responds to these orders by preparing for Mr. Low's visit to them later in the day. During his two-day stay Mr. Low receives several medications and three radiation treatments. He receives blood work to monitor his progress. All these treatments are made in response to orders by Dr. Good and are recorded in the medical record, along with the *progress notes* from each provider. The medical record serves as a primary form of communication among all the providers of care. They check the electronic medical record system regularly to look for new orders and to review the updated results of treatments and tests.

When Mr. Low is ready to be discharged, he is once again assessed by the nursing staff. A member of the nursing staff reviews his discharge orders from the physician and goes over instructions that Mr. Low should follow at home. Shortly after discharge, Dr. Good must dictate or record a *discharge summary* that outlines the course of treatment Mr. Low received. Once the record is flagged to indicate the patient has been discharged, the personnel in the Health Information Management Department assign codes to the diagnoses and procedures. These codes will be used by the Billing Department to file insurance claims.

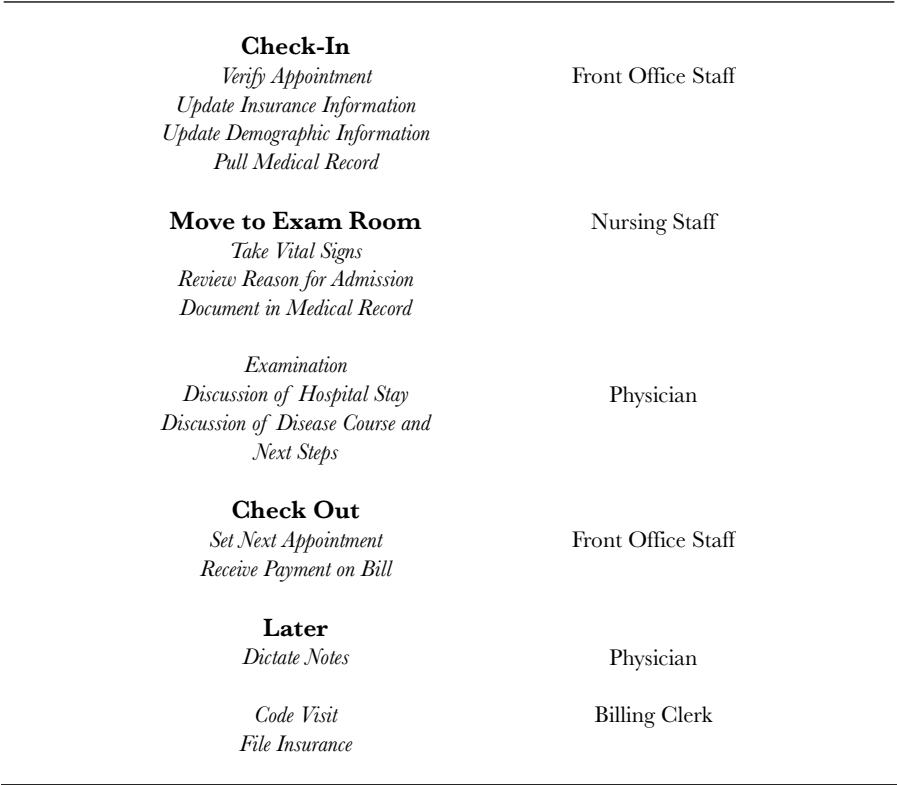
When the Billing Department receives the final codes for the records, it will submit the appropriate claims to the insurance companies. It is the Billing Department, or Patient Accounting Department, that manages the patient revenue cycle that begins with scheduling and ends when payments are posted. This department works closely with third-party payers and patients in collecting reimbursement for services provided.

Even in this extremely brief outline of a two-day hospital stay, you can see that patient care and the reimbursement for that care involve many individuals who need access to timely and accurate patient information. The coordination of care is essential to quality, and this coordination relies on the availability of information. Other hospital stays are longer; some are emergency admissions; some involve surgery. These stays will need information additional to that discussed in this section. However, the basic components will be essentially the same as those just described.

Mr. Low’s Physician’s Office Visit. An ambulatory care encounter is somewhat different from a hospital stay. Let’s follow Mr. Low again. This time we will describe his follow-up office visit with Dr. Good two weeks after his discharge from the hospital. Figure 1.4 is an outline of the process that Mr. Low followed during his office visit and the individuals who were responsible for each step in the process.

Dr. Good also maintains a medical record for Mr. Low, but his records are still mainly paper based. There is no direct link between Dr. Good’s and the hospital’s medical record systems. Fortunately, Dr. Good can access the hospital’s electronic medical record system from his office. He can view all the lab results, radiology reports, and discharge summaries for his patients. He chooses to print out these reports and file them in his patients’ paper medical records. Each medical record in Dr. Good’s office contains the general patient demographic and insurance information, an ongoing problem list, a summary of visits, and individual visit notes. These notes include entries by both the nursing staff and Dr. Good. The nursing staff record all their notes by hand. Dr. Good dictates his notes, which are subsequently transcribed by a professional medical transcriber. All phone calls and prescription information are also recorded in the record.

FIGURE 1.4. PHYSICIAN’S OFFICE VISIT PATIENT FLOW.



One significant difference between an ambulatory care visit, such as a physician's office visit, and a hospital stay is the scope of the episode of care. In an inpatient stay patients usually receive a course of treatment, with a definite admission point and discharge point. In an ambulatory care setting, particularly primary care physician visits, patients may have multiple problems and treatments that are ongoing. There may not be a definitive beginning or end to any one course of treatment. There are likely to be fewer care providers interacting with the patient at any given ambulatory care visit. There may, however, be more consultations and a need to coordinate care across organizations. All these characteristics make the clinical information needs of the inpatient setting and the ambulatory care setting somewhat different, but in each setting, this information is equally important to the provision of high-quality care.

Health care information systems and health care processes are closely entwined with one another. Health care processes require the use of data and information and they also produce or create information. Care providers must communicate with one another and often need to share patient information across organizations. The information produced by any one health care process may in turn be used by others. A true web of information sharing is needed.

Patient-Specific Data and Information—Administrative

As we have seen in the previous section, patient-specific clinical information is captured and stored as a part of the patient medical record. However, there is more to the story—health care organizations need to get paid for the care they provide and to plan for the efficient provision of services to ensure that their operations remain viable. In this section we will examine individual patient data and information used specifically for administrative purposes. Health care organizations need data to effectively perform the tasks associated with the patient revenue cycle, tasks such as scheduling, precertification and insurance eligibility determination, billing, and payment verification. To determine what data are needed, we can look, first, at two standard billing documents, the UB-92 (CMS-1450) and the CMS-1500. In addition, we will discuss the concept of a uniform data set and introduce the Uniform Hospital Discharge Data Set, the Uniform Ambulatory Care Data Set, and the Minimum Data Set for long-term care.

Data Needed to Process Reimbursement Claims

Generally, the health care organization's accounting or billing department is responsible for processing claims, which includes verifying insurance coverage, billing third-party payers (private insurance companies, Medicare, or Medicaid), and processing the claims as they are received. Depending on the type of service provided to the

patient, one of two standard billing forms will be submitted to the third-party payer. The CMS-1450, or UB-92, is submitted for inpatient, hospital-based outpatient, home health care, and long-term care services. The CMS-1500 is submitted for health care provider services, such as those provided by a physician's office.

UB-92. In 1975, the American Hospital Association (AHA) formed the National Uniform Billing Committee (NUBC, www.nubc.org), bringing together the major national provider and payer organizations with the purpose of developing a single billing form and standard data set that could be used for processing health care claims by institutions nationwide. The first *uniform bill* was the UB-82. It has since been modified and improved upon, resulting in the current UB-92 data set (see Exhibit 1.1). The UB-92 is the de facto hospital and other institution claim standard. It is required by the federal government and state governments and has been adopted across the United States by private third-party payers as well (NUBC, 1999).

CMS-1500. The National Uniform Claim Committee (NUCC, www.nucc.org) was created by the American Medical Association to provide a standardized data set for the noninstitutional health care community to use in the submission of claims (much as the NUBC has done for institutional providers). Members of this committee represent key provider and payer organizations, with the AMA appointing the committee chair. The standardized claim form developed and overseen by NUCC is the CMS-1500. This claim form has been adopted by the federal government, and like the UB-92 for institutional care, has become the de facto standard for all types of noninstitutional provider claims, such as those for physician services (see Exhibit 1.2).

It is important to recognize that both the UB-92 and the CMS-1500 claims forms incorporate standardized data sets. Regardless of the health care organization's location or the patient's insurance coverage, standard data elements are collected. In many states UB-92 data and CMS-1500 data must be reported to a central state agency responsible for aggregating and analyzing the state's health data. At the federal level the Centers for Medicare and Medicaid Services (CMS) aggregates the data from these claims forms for analyzing national health care reimbursement, clinical, and population trends. Having uniform data sets means that data can be compared, not only within organizations but within states and across the country.

Other Uniform Data Sets

Other uniform data sets have been developed for use in the United States. Three examples are the Uniform Hospital Discharge Data Set (UHDDS), the Uniform Ambulatory Care Data Set (ACDS), and the Minimum Data Set (MDS) used for long-term care. Each of these data sets shares two common purposes:

EXHIBIT 1.1. UNIFORM BILL: UB-92.

1		2										3 PATIENT CONTROL NO.										41TYPE OF BILL																																							
		5 FED. TAX NO.					6 STATEMENT COVERS PERIOD FROM					7 COV D.		8 ICD.		9 C4 D.		10 L-R D.		11																																									
b		12 PATIENT NAME															13 PATIENT ADDRESS																																												
		14 BIRTHDATE					15 SEX		16 MS		17 DATE		ADMISSION 18 HRI 19 TYPE 20 SRC			21 D HR		22 STAT		23 MEDICAL RECORD NO.					24		25		26		27		28		29		30		31																						
c		32 OCCURRENCE DATE					33 CODE		34 OCCURRENCE DATE					35 CODE		36 OCCURRENCE DATE					37 A B C		38					39 CODE					40 CODE					41 CODE					42																		
		32 OCCURRENCE DATE					33 CODE		34 OCCURRENCE DATE					35 CODE		36 OCCURRENCE DATE					37 A B C		38					39 CODE					40 CODE					41 CODE					42																		
d		42 REV. CD.					43 DESCRIPTION										44 HCPCS / RATES					45 SERV. DATE					46 SERV. UNITS					47 TOTAL CHARGES					48 NON-COVERED CHARGES					49																			
		42 REV. CD.					43 DESCRIPTION										44 HCPCS / RATES					45 SERV. DATE					46 SERV. UNITS					47 TOTAL CHARGES					48 NON-COVERED CHARGES					49																			
e		50 PAYER					51 PROVIDER NO.										52 REL INFO		53 ASG DEN		54 PRIOR PAYMENTS					55 EST. AMOUNT DUE					56																														
		50 PAYER					51 PROVIDER NO.										52 REL INFO		53 ASG DEN		54 PRIOR PAYMENTS					55 EST. AMOUNT DUE					56																														
f		57															DUE FROM PATIENT ▶															58																													
		57															DUE FROM PATIENT ▶															58																													
g		59 INSURED'S NAME										59 P. REL					60 CERT. - SSC - ID NO.										61 GROUP NAME										62 INSURANCE GROUP NO.																								
		59 INSURED'S NAME										59 P. REL					60 CERT. - SSC - ID NO.										61 GROUP NAME										62 INSURANCE GROUP NO.																								
h		63 TREATMENT AUTHORIZATION CODES										64 ESC					65 EMPLOYER NAME										66 EMPLOYER LOCATION																																		
		63 TREATMENT AUTHORIZATION CODES										64 ESC					65 EMPLOYER NAME										66 EMPLOYER LOCATION																																		
i		67 PRIN. DIAG. CD.					68 CODE					69 CODE					70 CODE					71 CODE					72 CODE					73 CODE					74 CODE					75 CODE					76 ADM. DIAG. CD.					77 E-CODE					78				
		67 PRIN. DIAG. CD.					68 CODE					69 CODE					70 CODE					71 CODE					72 CODE					73 CODE					74 CODE					75 CODE					76 ADM. DIAG. CD.					77 E-CODE					78				
j		79 P.C.					80					81					82					83					84					85					86					87					88														
		79 P.C.					80					81					82					83					84					85					86					87					88														
k		84 REMARKS															85 PROVIDER REPRESENTATIVE															86 DATE																													
		84 REMARKS															85 PROVIDER REPRESENTATIVE															86 DATE																													

1. To identify the data elements that should be collected for each patient, and
2. To provide uniform definitions for common terms and data elements [LaTour, 2002, p. 123].

The UHDDS is the oldest uniform data set used in the United States. An early version was developed in 1969 by the National Center for Health Statistics. In 1974, the federal government adopted the UHDDS definitions as the standard for the Medicare and Medicaid programs. The UHDDS has been revised several times. The current version includes the data elements listed in Figure 1.5.

The ACDS was approved by the National Committee on Vital and Health Statistics in 1989. The goal of the ACDS is to improve the data collected in ambulatory and outpatient settings. The ACDS has not, however, been incorporated into federal rules or regulations. It remains a recommended rather than a required data set.

The MDS for long-term care is a federally mandated standard assessment tool that is used to collect demographic and clinical information about long-term care facility residents. It is an extensive data set with detailed data elements in twenty major categories. The MDS provides a structured way to organize resident information so that an effective care plan can be developed (LaTour, 2002).

Patient-Specific Data and Information— Combining Clinical and Administrative

As we have discussed in earlier sections of this chapter, diagnostic and procedural information is captured during the patient encounter to track clinical progress and to document care for reimbursement and other administrative purposes. This diagnostic and procedural information is initially captured in narrative form through the physicians' and other health care providers' documentation in the patient record. This documentation is subsequently translated into numerical codes. Coding facilitates the classification of diagnoses and procedures not only for reimbursement purposes but also for clinical research and comparative studies.

Two major coding systems are employed by health care providers today:

- ICD-9-CM (International Classification of Diseases, ninth revision, clinical modification—modified for use in the United States), published by the National Center for Healthcare Statistics
- CPT (Current Procedural Terminology), published by the American Medical Association

Use of these systems is required by the federal government for reimbursement, and they are recognized by health care agencies both nationally and internationally.

EXHIBIT 1.2. CLAIM FORM: CMS-1500.

PLEASE
DO NOT
STAPLE
IN THIS
AREA

APPROVED OMB-0938-0008

HEALTH INSURANCE CLAIM FORM									
☐ PICA ☐ PICA									
1. MEDICARE ☐ MEDICAID ☐ CHAMPUS ☐ CHAMPVA ☐ GROUP HEALTH PLAN ☐ FECA ☐ OTHER ☐			1a. INSURED'S I.D. NUMBER (FOR PROGRAM IN ITEM 1)						
2. PATIENT'S NAME (Last Name, First Name, Middle Initial)			3. PATIENT'S BIRTH DATE MM DD YY			4. INSURED'S NAME (Last Name, First Name, Middle Initial)			
5. PATIENT'S ADDRESS (No., Street) CITY STATE ZIP CODE TELEPHONE (Include Area Code)			6. PATIENT RELATIONSHIP TO INSURED Self ☐ Spouse ☐ Child ☐ Other ☐			7. INSURED'S ADDRESS (No., Street) CITY STATE ZIP CODE TELEPHONE (INCLUDE AREA CODE)			
8. PATIENT STATUS Single ☐ Married ☐ Other ☐			9. OTHER INSURED'S NAME (Last Name, First Name, Middle Initial)			10. IS PATIENT'S CONDITION RELATED TO:			
11. INSURED'S POLICY GROUP OR FECA NUMBER			12. IS THERE ANOTHER HEALTH BENEFIT PLAN? ☐ YES ☐ NO			13. INSURED'S DATE OF BIRTH MM DD YY			
14. OTHER INSURED'S POLICY OR GROUP NUMBER			15. EMPLOYMENT? (CURRENT OR PREVIOUS) ☐ YES ☐ NO			16. EMPLOYER'S NAME OR SCHOOL NAME			
17. OTHER INSURED'S DATE OF BIRTH MM DD YY			18. AUTO ACCIDENT? ☐ YES ☐ NO			19. INSURANCE PLAN NAME OR PROGRAM NAME			
20. EMPLOYER'S NAME OR SCHOOL NAME			21. OTHER ACCIDENT? ☐ YES ☐ NO			22. IS THERE ANOTHER HEALTH BENEFIT PLAN? ☐ YES ☐ NO			
23. INSURANCE PLAN NAME OR PROGRAM NAME			24. RESERVED FOR LOCAL USE			25. IS THERE ANOTHER HEALTH BENEFIT PLAN? ☐ YES ☐ NO			
READ BACK OF FORM BEFORE COMPLETING & SIGNING THIS FORM.									
12. PATIENT'S OR AUTHORIZED PERSON'S SIGNATURE: I authorize the release of any medical or other information necessary to process this claim, I also request payment of government benefits either to myself or to the party who accepts assignment below.					13. INSURED'S OR AUTHORIZED PERSON'S SIGNATURE: I authorize payment of medical benefits to the undersigned physician or supplier for services described below.				
SIGNED _____ DATE _____					SIGNED _____				
14. DATE OF CURRENT ILLNESS (First symptom) OR INJURY (Accident) OR PREGNANCY (LMP)					15. IF PATIENT HAS HAD SAME OR SIMILAR ILLNESS, GIVE FIRST DATE				
17. NAME OF REFERRING PHYSICIAN OR OTHER SOURCE					17a. LD, NUMBER OF REFERRING PHYSICIAN				
19. RESERVED FOR LOCAL USE					20. OUTSIDE LAB? ☐ YES ☐ NO				
21. DIAGNOSIS OR NATURE OF ILLNESS OR INJURY, (RELATE ITEMS 1,2,3 OR 4 TO ITEM 24E BY LINE)					22. MEDICAID RESUBMISSION CODE				
1. _____					23. PRIOR AUTHORIZATION NUMBER				
2. _____					24. _____				
24. A. DATE(S) OF SERVICE, FROM TO MM DD YY MM DD YY					B. PLACE OF SERVICE				
C. TYPE OF SERVICE					D. PROCEDURES, SERVICES, OR SUPPLIES (Explain Unusual Circumstances) CPT/HCPCS MODIFIER				
E. DIAGNOSIS CODE					F. \$ CHARGES				
G. DAYS OR UNITS					H. EMG				
I. COB					J. RESERVED FOR LOCAL USE				
25. FEDERAL TAX I.D. NUMBER					26. PATIENT'S ACCOUNT NO.				
27. ACCEPT ASSIGNMENT? (For gov. claims, see back)					28. TOTAL CHARGE				
29. AMOUNT PAID					30. BALANCE DUE				
31. SIGNATURE OF PHYSICIAN OR SUPPLIER INCLUDING DEGREES OR CREDENTIALS (I certify that the statements on the reverse apply to this bill and are made a part thereof.)					32. NAME AND ADDRESS OF FACILITY WHERE SERVICES WERE RENDERED (If other than home or office)				
33. PHYSICIAN'S, SUPPLIER'S BILLING NAME, ADDRESS, ZIP CODE & PHONE #					PIN# GRP#				

(APPROVED BY AMA COUNCIL ON MEDICAL SERVICE 8/88)

PLEASE PRINT OR TYPE

FORM HCFA-1500 (12-90), FORM RRB-1500, FORM OWCP-1500

ICD-9-CM

The ICD-9-CM classification system is derived from the International Classification of Diseases, ninth revision, which was developed by the World Health Organization to capture disease data. ICD-9-CM is used in the United States to code not only disease information but also procedure information. An update to the ICD-9-CM is published each year. This publication is considered a federal government document whose contents may be used freely by others. However, multiple companies republish this government document in easier-to-use, annotated, formally copyrighted versions. The precursors to the current ICD system were developed to allow morbidity (illness) and mortality (death) statistics to be compared across nations. ICD-9-CM coding, however, has come to play a major role in reimbursement to hospitals. Since 1983, it has been used for determining the *diagnosis related group (DRG)* into which a patient is assigned. DRGs are the basis for determining appropriate inpatient reimbursements for Medicare, Medicaid, and many other health care insurance beneficiaries. Accurate ICD-9-CM coding has as a consequence become vital to accurate institutional reimbursement. Figure 1.6 is an excerpt from the ICD-9-CM classification system. It shows the system in its text form, but large health care organizations generally use *encoders*, computer applications that facilitate accurate coding. Whether a book or text file or encoder is used, the classification system is the same.

It should be noted that a tenth revision of the ICD has been published by the World Health Organization and is widely used in countries other than the United States. The U.S. government has published draft modifications of ICD-10, but these have not yet been finalized and adopted for use in this country. The original adoption date for ICD-10-CM was to be late 2001, but as of this writing it has not been released. The conversion from ICD-9-CM to ICD-10-CM will be a tremendous undertaking for health care organizations. ICD-10 includes substantial increases in content and many structural changes. When the U.S. modification is released, all health care providers will need to adjust their systems to reflect the conversion from ICD-9-CM to ICD-10-CM.

CPT

The American Medical Association (AMA) publishes an updated Current Procedural Terminology each year. Unlike ICD-9-CM, CPT is copyrighted, with all rights to publications and distribution held by the AMA. CPT was first developed and published in 1966. The stated purpose for developing CPT was to provide a uniform language for describing medical and surgical services. In 1983, however, the government adopted CPT, in its entirety, as the major component (known as Level 1) of the Healthcare Common Procedural Coding System (HCPCS). Since then CPT has become the standard for

FIGURE 1.5. UHDDS ELEMENTS AND DEFINITIONS.

UHDDS elements as adopted in 1986 are:

1. **Personal identification:** the unique number assigned to each patient within a hospital that distinguishes the patient and his or her hospital record from all others in that institution
2. **Sex:** male or female
3. **Race:** White, Black, Asian or Pacific Islander, American Indian/Eskimo/Aleut, or other
4. **Ethnicity:** Spanish origin/Hispanic, Non-Spanish origin/Non-Hispanic
5. **Residence:** zip code, code for foreign residence
6. **Hospital identification:** a unique institutional number within a data collection system
- 7–8. **Admission and discharge dates:** month, day, and year of both admission and discharge. An inpatient admission begins with the formal acceptance by a hospital of a patient who is to receive physician, dentist, or allied services while receiving room, board, and continuous nursing services. An inpatient discharge occurs with the termination of the room, board, and continuous nursing services, and the formal release of an inpatient by the hospital.
- 9–10. **Attending physician and operating physician:** each physician must have a unique identification number within the hospital. The attending physician and the operating physician (if applicable) are to be identified.

Attending physician: the clinician who is primarily and largely responsible for the care of the patient from the beginning of the hospital episode.

Operating physician: the clinician who performed the principal procedure (see item 12 for definition of a principal procedure)
11. **Diagnoses:** all diagnoses that affect the current hospital stay

Principal diagnosis is designated and defined as the condition established after study to be chiefly responsible for occasioning the admission of the patient to the hospital for care. **Other diagnoses** are designated and defined as all conditions that coexist at the time of admission, that develop subsequently, or that affect the treatment received or length of stay. Diagnoses that relate to an earlier episode that have no bearing on the current hospital stay are to be excluded.

- 12. Procedure and date:** all significant procedures are to be reported. A significant procedure is one that is surgical in nature, or carries a procedural risk, or carries an anesthetic risk, or requires specialized training. For significant procedures, the identity (by unique number within the hospital) of the person performing the procedure and the data must be reported. When more than one procedure is reported, the principal procedure is to be designated. In determining which of several procedures is principal, the following criteria apply:

The principal procedure is one that was performed for **definitive treatment** rather than one performed for diagnostic or exploratory purposes, or was necessary to take care of a complication. If there appear to be two procedures that are principal, then the one most related to the principal diagnosis should be selected as the principal procedure. For reporting purposes, the following definition should be used: surgery includes incision, excision, amputation, introduction, endoscopy, repair, destruction, suture, and manipulation.

- 13. Disposition of patient:** discharged to home (routine discharge); left against medical advice; discharged to another short-term hospital; discharged to a long-term institution; died, or other
- 14. Expected payer** for most of this bill (anticipated financial guarantor for services): this refers to the single major source that the patient expects will pay for his or her bill, such as Blue Cross, other insurance companies, Medicare, Medicaid, Workers' Compensation, other government payers, self-pay, no-charge (free, charity, special research, or teaching), or other.

Source: Dougherty, 2001, p. 72.

physician's office, outpatient, and ambulatory care coding for reimbursement purposes. There were nearly 8,000 CPT codes in the fourth edition. A fifth edition is currently being developed (American Medical Association, 2005). Figure 1.7 is a patient encounter form with examples of HCPCS/CPT codes.

Coding Standards

As coding has become intimately linked to reimbursement, directly determining the amount of money a health care organization can receive for a claim from insurers, the government has increased its scrutiny of coding practices. There are official guidelines for accurate coding, and health care facilities that do not adhere to these guidelines are liable to charges of fraudulent coding practices. In addition the Department of Health

FIGURE 1.6. EXCERPT FROM THE ICD-9-CM DISEASE INDEX.**ARTHROPATHIES AND RELATED DISORDERS (710-719)****Excludes: disorders of spine (720.0-724.9)****710 Diffuse diseases of connective tissue**

Includes: all collagen diseases whose effects are not mainly confined to a single system

Excludes: those affecting mainly the cardiovascular system, i.e., polyarteritis nodosa and allied conditions (446.0-446.7)

- 710.0 Systemic lupus erythematosus
 - Disseminated lupus erythematosus
 - Libman-Sacks disease

Use additional code to identify manifestation, as:

- endocarditis (424.91)
- nephritis (583.81)
- chronic (582.81)
- nephrotic syndrome (581.81)

Excludes: lupus erythematosus (discoid) NOS (695.4)

- 710.1 Systemic sclerosis
 - Acrosclerosis
 - CRST syndrome
 - Progressive systemic sclerosis
 - Scleroderma

Use additional code to identify manifestation, as:

- lung involvement (517.2)
- myopathy (359.6)

Excludes: circumscribed scleroderma (701.0)

- 710.2 Sicca syndrome
 - Keratoconjunctivitis sicca
 - Sjögren's disease

- 710.3 Dermatomyositis
 - Poikilodermatomyositis
 - Polymyositis with skin involvement

- 710.4 Polymyositis

- 710.5 Eosinophilia myalgia syndrome
 - Toxic oil syndrome

Use additional E to identify drug, if drug induced

- 710.8 Other specified diffuse diseases of connective tissue
 - Multifocal fibrosclerosis (idiopathic) NEC
 - Systemic fibrosclerosing syndrome

- 710.9 Unspecified diffuse connective tissue disease
 - Collagen disease NOS

Source: National Center for Health Statistics, 2004.

FIGURE 1.7. PATIENT ENCOUNTER FORM.

Pediatric Associates P.A. 123 Children's Avenue Anytown, USA

Office Visits

99211 Estab Pt—minimal	\$	Preventive Medicine—New	\$
99212 Estab Pt—focused		99381 Prev Med 0–1 years	
99213 Estab Pt—expanded		99382 Prev Med 1–4 years	
99214 Estab Pt—detailed		99383 Prev Med 5–11 years	
99215 Estab Pt—high complexity		99384 Prev Med 12–17 years	
		99385 Prev Med 18–39 years	
99201 New Pt—problem focused			
99202 New Pt—expanded		Preventive Medicine—Established	
99203 New Pt—detailed		99391 Prev Med 0–1 years	
99204 New Pt—moderate complexity		99392 Prev Med 1–4 years	
99205 New Pt—high complexity		99393 Prev Med 5–11 years	
		99394 Prev Med 12–17 years	
99050 After Hours		99395 Prev Med 18–39 years	
99052 After Hours—after 10 pm			
99054 After Hours—Sundays and Holidays		99070 10 Arm Sling	
		99070 11 Sterile Dressing	
Outpatient Consult		99070 45 Cervical Cap	
99241 99242 99243 99244 99245			

Immunizations, Injections, and Office Laboratory Services

90471 Adm of Vaccine 1		81000 Urinalysis w/ micro	
90472 Adm of Vaccine >1		81002 Urinalysis w/o micro	
90648 HIB		82270 Hemocult Stool	
90658 Influenza		82948 Dextrostix	
90669 Prevnar	\$	83655 Lead Level	\$
90701 DTP		84030 PKU	
90702 DT		85018 Hemoglobin	
90707 MMR		87086 Urine Culture	
90713 Polio Injection		87081 Throat Culture	
90720 DTP/HIB		87205 Gram Stain	
90700 DTaP		87208 Ova Smear (pin worm)	
90730 Hepatitis A		87210 Wet Prep	
90733 Meningococcal		87880 Rapid Strep	
90744 Hepatitis B 0–11			
90746 Hepatitis B 18+ years			

Diagnosis**Patient Name****No.****Date****Time****Address****DOB****Name of Insured****ID****Insurance Company****Return Appointment** _____

and Human Services Office of Inspector General (HHS OIG) publishes compliance guidelines to facilitate health care organizations' adherence to ethical and legal coding practices. The OIG is responsible for (among other duties) investigating fraud involving government health insurance programs. More specific information about compliance guidelines can be found on the OIG Web site (www.oig.hhs.gov) (HHS OIG, 2004).

Aggregate Health Care Data and Information—Clinical

In the previous section we examined different sets of clinical and administrative data that are collected during or in the time closely surrounding the patient encounter. Patient records, uniform billing information, and discharge data sets are the main sources of the data that go into the literally hundreds of aggregate reports or queries that are developed and used by providers and executives in health care organizations. Think of these source data as one or more data repositories, with each data element available to health care providers and executives. What can these data tell you about the organization and the care provided to patients? How can you process these data into meaningful information? The number of aggregate reports that could be developed from patient records or patient accounting information is practically limitless, but there are some common categories of clinical, administrative, and combined reports that the health care executive will likely encounter. We will discuss a few of these in this and the following sections.

On the clinical side, disease indexes and specialized registers are often used.

Disease and Procedure Indexes

Health care organization management often wants to know summary information about a particular disease or treatment. Examples of questions that might be asked are: What is the most common diagnosis in the facility? What percentage of diabetes patients are African American? What is the most common procedure performed on patients admitted with gastritis (or heart attack or any other diagnosis)? Traditionally, such questions have been answered by looking in disease and procedure indexes. Prior to the widespread use of databases and computers, disease and procedure indexes were large card catalogs or books that kept track of the numbers of diseases treated and procedures occurring in a facility by disease and procedure ICD codes. Now that databases and computers are common, the disease and procedure index function is generally handled as a component of the patient medical record system or the registration and discharge system. The retrieval of information related to diseases and procedures is still based on ICD-9-CM

Many other types of aggregate clinical reports are used by health care providers and executives. The easy-to-use ad hoc reporting that is available with databases today gives providers and executives access to any number of summary reports based on the data elements collected during the patient encounter.

Aggregate Health Care Data and Information—Administrative

Just as with clinical aggregate reports, a limitless number of reports can be created for administrative functions from today's databases and data repositories. Commonly used administrative aggregate reports include basic health care statistical reports, claims denial reports, and cost reports. (In keeping with our focus on information unique to health care we will not discuss traditional income statements, cash flow statements, or other general accounting reports.) Two basic types are described in this section: Medicare cost reports and basic health care statistical reports.

Medicare Cost Reports

Exhibit 1.3 is a portion of a Medicare cost report for a skilled nursing facility (CMS-2552-96). Medicare cost reports are filed annually by all hospitals, home health agencies, skilled nursing facilities, and hospices that accept Medicare or Medicaid. These reports must be filed within a specified time after the end of the fiscal year and are subject to scrutiny via compliance audits. The cost report contains such provider information as facility characteristics, utilization data, costs and charges by cost center (in total and for Medicare), Medicare settlement data, and financial statement data. Preparation instructions and the actual forms can be found on the CMS Web site (www.cms.gov). Medicare cost reports are used by CMS not only to determine portions of an individual facility's reimbursement but also to determine Medicare rate adjustments, cost limits, and various wage indexes.

Health Care Statistics

The categories of statistics that are routinely gathered for health care executives or others include

- *Census statistics.* These data reveal the number of patients present at any one time in a facility. Several commonly computed rates are based on this census data, including the average daily census and bed occupancy rates.
- *Discharge statistics.* This group of statistics is calculated from data accumulated when patients are discharged. Some commonly computed rates based on discharge statistics are average length of stay, death rates, autopsy rates, infection rates, and consultation rates.

General health care statistics are frequently used to describe the characteristics of the patients within an organization. They may also provide a basis for planning and monitoring patient services.

EXHIBIT 1.3. SECTION OF A MEDICARE COST REPORT FOR A SKILLED NURSING FACILITY.

3690 (Cont.)		CMS FORM-2552-96			06-03	
COMPUTATION OF INPATIENT OPERATING COST		PROVIDER NO.:	COMPONENT NO.:	PERIOD: FROM _____ TO _____	WORKSHEET D-1, PARTS III & IV	
Check applicable boxes	☐ Title V - I/P ☐ Title XVIII, Part A ☐ Title XIX - I/P	☐ Hospital ☐ Subprovider ☐ SNF	☐ NF ☐ ICF/MR	☐ PPS ☐ TEFRA ☐ Other		
PART III - SKILLED NURSING FACILITY, OTHER NURSING FACILITY, AND ICF/MR ONLY						
66	Skilled nursing facility/other nursing facility/ICF/MR routine service cost (line 37)					66
67	Adjusted general inpatient routine service cost per diem (line 66 ÷ line 2)					67
68	Program routine service cost (line 9 x line 67)					68
69	Medically necessary private room cost applicable to Program (line 14 x line 35)					69
70	Total Program general inpatient routine service costs (line 68 + line 69)					70
71	Capital-related cost allocated to inpatient routine service costs (from Worksheet B, sum of Parts II and III, column 27)					71
72	Per diem capital-related costs (line 71 ÷ line 2)					72
73	Program capital-related costs (line 9 x line 72)					73
74	Inpatient routine service cost (line 70 minus line 73)					74
75	Aggregate charges to beneficiaries for excess costs (from provider records)					75
76	Total Program routine service costs for comparison to the cost limitation (line 74 minus line 75)					76
77	Inpatient routine service cost per diem limitation					77
78	Inpatient routine service cost limitation (line 9 x line 77)					78
79	Reasonable inpatient routine service costs (see instructions)					79
80	Program inpatient ancillary services (see instructions)					80
81	Utilization review - physician compensation					81
82	Total Program inpatient operating costs (sum of lines 79 through 81)					82
PART IV - COMPUTATION OF OBSERVATION BED PASS THROUGH COST						
83	Total observation bed days (see instructions)					83
84	Adjusted general inpatient routine cost per diem (line 27 ÷ line 2)					84
85	Observation bed cost (line 83 x line 84) (see instructions)					85
COMPUTATION OF OBSERVATION BED PASS THROUGH COST						
		Cost	Routine Cost (from line 27)	col. 1 ÷ col. 2	Total Observation Bed Cost (from line 85)	Observation Bed Pass Through Cost (col. 3 x col. 4) (see instructions)
		1	2	3	4	5
86	Old capital-related cost					86
87	New capital-related cost					87
88	Non Physician Anesthetist					88
89	Medical Education					89

FORM CMS-2552-96 (11/98) (INSTRUCTIONS FOR THIS WORKSHEET ARE PUBLISHED IN CMS PUB. 15-11, SECTIONS 3622.3-3622.4)

Aggregate Health Care Data and Information—Combining Clinical and Administrative

Health care executives are often interested in aggregate reports that combine clinical and administrative data. Ad hoc statistical reports and trend analyses may draw from both clinical and administrative data sources, for example. These reports may be used for the purpose of improving customer service, quality of patient care, or overall operational efficiency. Examples of aggregate data that relate to customer service are the average time it takes to get an appointment at a clinic and the average referral volume by physician. Quality of care aggregate data take many forms, revealing such things as infection rates and unplanned returns to the operating room. Cost per case, average reimbursement by DRG, and staffing levels by patient acuity are examples of aggregate data that could be used to improve efficiency. These examples represent only a few uses for combined aggregate data. Again, with today's computerized clinical and administrative databases, any number of ad hoc queries, statistical reports, and trend analyses should be readily available to health care executives. Health care executives need to know what source data are collected and must be able to trust in data accuracy. Executives should be creative in designing aggregate reports to meet their decision-making needs.

External Data and Information—Comparative

Comparative data and information are used for both clinical and administrative purposes by health care organizations.

Outcome Measures and Balanced Scorecards

Comparative data and information are often aligned with organizations' quality improvement efforts. For example, an organization might collect data on specific outcomes measures and then use this information in a benchmarking process. *Outcomes measures* are the measurable results of a process. This could be a clinical process, such as a particular treatment, or an administrative process, such as a claims filing. Outcomes measures can be applied to individuals or groups. An example of a simple clinical outcomes measure is the percentage of similar lab results that occur within a month for a particular medical group. An example of an administrative measure is the percentage of claims denied by Medicare during one month. Implicit in the idea of measuring outcomes is that they can be usefully compared over time or against a set standard. The process of comparing one or more

outcomes measures against a standard is called *benchmarking*. Outcomes measures and benchmarking may be limited to internally set standards; however, frequently they are involved in comparisons with externally generated benchmarks or standards.

Balanced scorecards represent another method for measuring performance in health care organizations. The concept of the balanced scorecard relates to the need for executives to design measurement systems that are aligned with their organization's strategy goals (Kelly, 2003). In balanced scorecard systems, multiple measures are examined, rather than the one set of outcomes measures that is common in traditional benchmarking. Suppose a health care organization uses "lowest-cost service in the region" as an outcome measure for benchmarking its performance against that of like facilities in the region. The organization does very well over time on this measure. However, you can see that it may be ignoring some other important performance indicators. What about patient satisfaction? Employee morale? Patient health outcomes? Balanced scorecards employ multiple measures along several dimensions to ensure that the organization is performing well across the board. The *clinical value compass* is a similar method for measuring clinical process across multiple dimensions (Kelly, 2003).

Comparative Health Care Data Sets

Organizations may select from many publicly and privately available health care data sets for benchmarking. A few of the more commonly accessed data sets are listed in Figure 1.9. We will take a closer look at three of the most commonly used measures: HEDIS, ORYX, and CMS data.

HEDIS. The mission of the National Committee for Quality Assurance (NCQA, 2004) is "to provide information that enables purchasers and consumers of managed health care to distinguish among plans based on quality, thereby allowing them to make more informed health care purchasing decisions." NCQA's efforts are organized around two activities, accreditation and performance measurement. (We will discuss the accreditation activity in Chapter Three.) To facilitate these activities NCQA developed the Health Plan Employer Data and Information Set (HEDIS) in the late 1980s. HEDIS data have been used to calculate national performance statistics and benchmarks as well as to set standards for measures used by NCQA's accreditation program. Exhibit 1.4 is a summary list of the 2004 HEDIS measures as they apply to Medicaid, commercial health plans, Medicare, and preferred provider organizations (PPOs). Specific indicators in each measure category are measured for each health plan.

The NCQA Web site offers an interactive tool for obtaining *report cards* on specific health plans that have undergone NCQA accreditation. These report cards use HEDIS data as the basis of comparison. In addition, employers and other groups providing

**FIGURE 1.9. SOURCES OF COMPARATIVE DATA FOR
HEALTH CARE MANAGERS.**

Patient Satisfaction

- Picker Survey (National Research Corporation) www.patientexperiencestandard.org
- Press Ganey Associates www.nationalresearch.com
- The Gallup Organization www.gallup.com

Practice Patterns

- Leatherman, S., and McCarthy, D. *Quality of Healthcare in the United States: A Chartbook*. New York: The Commonwealth Fund.
- The Center for the Evaluative Clinical Sciences, Dartmouth Medical School. (1996). *The Dartmouth Atlas of Healthcare*. Chicago: American Hospital Publishing Company.

Health Plans

- National Committee for Quality Assurance (NCQA) HEDIS measures www.ncqa.org

Clinical Indicators

- JCAHO ORYX measures www.jcaho.org/pms
- Centers for Medicare and Medicaid Services (CMS), Medicare clinical indicators www.cms.gov

Population Measures

- State and local health departments
- Centers for Disease Control and Prevention, National Center for Health Statistics www.cdc.gov/nchs
- Centers for Medicare and Medicaid Services (CMS) www.cms.gov

Source: Used with permission from *Applying Quality Management in Healthcare*, by Diane Kelly (Chicago: Health Administration Press, 2003), p. 136.

health benefits may use HEDIS data for comparison purposes. Table 1.2 is an example of HEDIS report data. This particular report compares one of the health plans available through the Federal Employees Health Benefit Program (FEHBP) with all the other available plans. HEDIS data are also used in a program called Quality Compass, which allows health plans, purchasers, consultants, and the media to compare health plan performance. (Health plans must give permission before their HEDIS data can be used in this program.) NCQA (2004) also collects Medicare HEDIS data on behalf of CMS and Medicaid HEDIS data on behalf of many state agencies.

ORYX. JCAHO's ORYX initiative integrates outcomes and other performance measurement data into the hospital accreditation process. On July 1, 2002, accredited hospitals began collecting data on four initial core measure sets, focused on acute myocardial infarction, heart failure, community acquired pneumonia, and pregnancy and related conditions. Other sets of core measures are currently being developed, and beginning in 2004, these data will be used by JCAHO for focusing on-site survey evaluation activities. A hospital seeking accreditation is required to select from the ORYX core measure sets based on the services it provides. However, if the hospital does not provide services in any of the core measurement areas, it can select other measures that meet JCAHO's approval. Comparisons of health care organizations' core measures will eventually be made publicly available on the JCAHO Web site. The current ORYX measures for treatment of heart failure, for example, include the following two indicators (out of a total of four):

Performance Measure Name: (HF-1) Discharge instructions

Description: Heart failure patients discharged home with written instructions or educational material given to patient or caregiver at discharge or during the hospital stay addressing all of the following: activity level, diet, discharge medications, follow-up appointment, weight monitoring, and what to do if symptoms worsen.

Numerator: Heart failure patients with documentation that they or their caregivers were given written discharge instruction or other educational material addressing all of the following: activity level, diet, discharge medications, follow-up appointment, weight monitoring, and what to do if symptoms worsen.

Denominator: Heart failure patients discharged home.

Data Reported as: Aggregate rate generated from count data reported as a proportion.

Improvement Noted as: An increase in the rate.

EXHIBIT 1.4. HEDIS 2004 SUMMARY TABLE OF MEASURES AND PRODUCT LINES.

HEDIS® 2004 Measures	Applicable to:			
	Medicaid	Commercial	Medicare	PPO
Effectiveness of Care				
Childhood Immunization Status	X	X		
Adolescent Immunization Status	X	X		
Appropriate Treatment for Children With Upper Respiratory Infection	X	X		
Appropriate Testing for Children With Pharyngitis	X	X		
Colorectal Cancer Screening		X	X	
Breast Cancer Screening	X	X	X	
Cervical Cancer Screening	X	X		
Chlamydia Screening in Women	X	X		
Osteoporosis Management in Women Who Had a Fracture			X	
Controlling High Blood Pressure	X	X	X	
Beta-Blocker Treatment After a Heart Attack	X	X	X	
Cholesterol Management After Acute Cardiovascular Event	X	X	X	
Comprehensive Diabetes Care	X	X	X	
Use of Appropriate Medications for People With Asthma	X	X		
Follow-Up After Hospitalization for Mental Illness	X	X	X	
Antidepressant Medication Management	X	X	X	
Medical Assistance With Smoking Cessation	X	X	X (ASTQ only)	
Flu Shots for Adults Age 50–64		X		
Flu Shots for Older Adults			X	
Pneumonia Vaccination Status for Older Adults			X	
Medicare Health Outcomes Survey			X	
Management of Urinary Incontinence in Older Adults			X	
Access/Availability of Care				
Adults' Access to Preventive/ Ambulatory Health Services	X	X	X	
Children's and Adolescents' Access to Primary Care Practitioners	X	X		
Prenatal and Postpartum Care	X	X		
Annual Dental Visit	X			
Initiation and Engagement of Alcohol and Other Drug Dependence Treatment	X	X	X	
Claims Timeliness	X	X	X	X
Call Answer Timeliness	X	X	X	X
Call Abandonment	X	X	X	X
Satisfaction With the Experience of Care				
CAHPS® 3.0H Adult Survey	X	X		
CAHPS® 3.0H Child Survey	X	X		X
ECHO™ 3.0H Survey for MBHOs		X (MBHO only)		

HEDIS® 2004 Measures	Applicable to:			
	Medicaid	Commercial	Medicare	PPO
Health Plan Stability				
Practitioner Turnover	X	X	X	
Years in Business/Total Membership	X	X	X	
Use of Services				
Frequency of Ongoing Prenatal Care	X			
Well-Child Visits in the First 15 Months of Life	X	X		
Well-Child Visits in the Third, Fourth, Fifth and Sixth Years of Life	X	X		
Adolescent Well-Care Visit	X	X		
Frequency of Selected Procedures	X	X	X	
Inpatient Utilization—General Hospital/Acute Care	X	X	X	
Ambulatory Care	X	X	X	
Inpatient Utilization—Nonacute Care	X	X	X	
Discharge and Average Length of Stay—Maternity Care	X	X		
Cesarean Section Rate	X	X		
Vaginal Birth After Cesarean Rate (VBAC Rate)	X	X		
Births and Average Length of Stay, Newborns	X	X		
Mental Health Utilization—Inpatient Discharges and Average Length of Stay	X	X	X	
Mental Health Utilization—Percentage of Members Receiving Services	X	X	X	
Chemical Dependency Utilization—Inpatient Discharges and Average Length of Stay	X	X	X	
Chemical Dependency Utilization—Percentage of Members Receiving Services	X	X	X	
Identification of Alcohol and Other Drug Services	X	X	X	
Outpatient Drug Utilization	X	X	X	
Health Plan Descriptive Information				
Board Certification	X	X	X	
Total Enrollment by Percentage	X	X	X	
Enrollment by Product Line	X	X	X	
Unduplicated Count of Medicaid Members	X			
Diversity of Medicaid Membership	X			
Weeks of Pregnancy at Time of Enrollment in the MCO	X			

Source: <http://www.neqa.org/Programs/HEDIS/Hedis%202004%20Summary%20Table.pdf>

Performance Measure Name: (HF-2) LVF assessment

Description: Heart failure patients with documentation in the hospital record that left ventricular function (LVF) was assessed before arrival, during hospitalization, or is planned for after discharge.

Numerator: Heart failure patients with documentation in the hospital record that LVF was assessed before arrival, during hospitalization, or is planned for after discharge.

Denominator: Heart failure patients.

Data Reported as: Aggregate rate generated from count data reported as a proportion.

Improvement Noted as: An increase in the rate [JCAHO, 2004b].

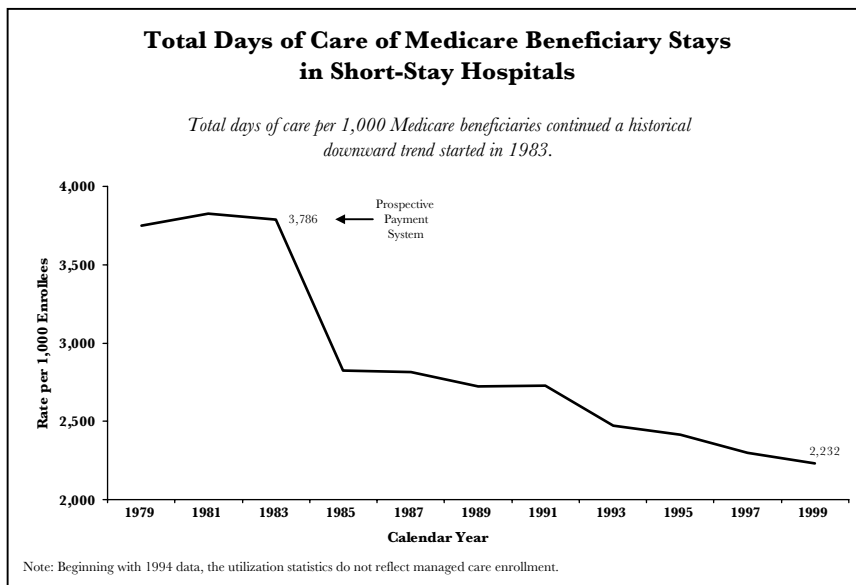
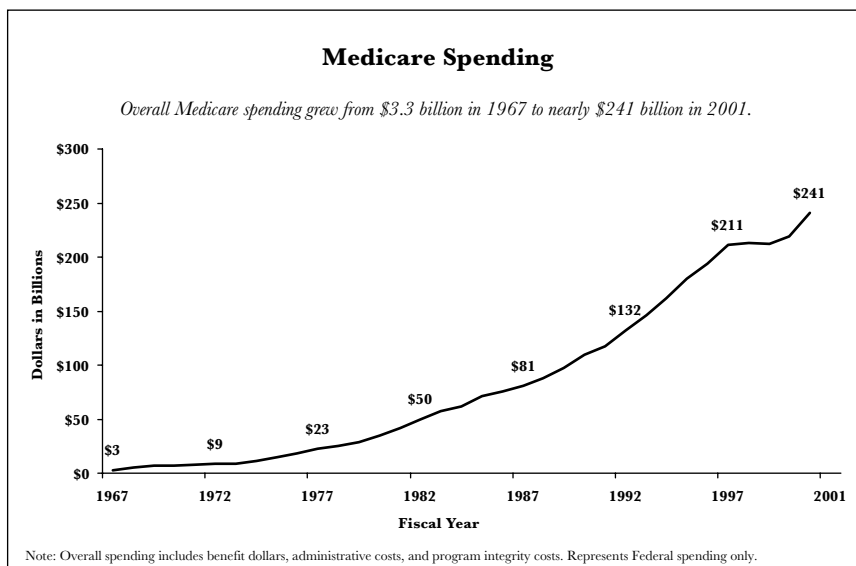
CMS. A wide range of quality improvement data, population data, and cost data is available to health care organizations from the Centers for Medicare and Medicaid Services (CMS). CMS routinely publishes summary reports related to reimbursement, as well as selected quality indicators. The CMS Web site provides free access to these data sets and summary reports. Figure 1.10 shows two of the dozens of charts available. Many other summary reports and raw data sets are also available.

**TABLE 1.2. FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM:
HEDIS QUALITY MEASURES.**

Description	Average All Plans	This Plan
Antidepressant medication management		
1. Optimal practitioner contact—the percentage of members 18 and older who were diagnosed with a new episode of depression, treated with an antidepressant medication, and who had at least 3 follow-up contacts with a primary care practitioner or mental health practitioner during the 84-day (12 week) acute treatment phase	20%	22%
2. Acute treatment phase—the percentage of members 18 and older . . . who remained on an antidepressant drug during the entire 84-day (12-week) acute treatment phase	58	61
3. Continuation treatment phase—the percentage of members 18 and older . . . who remained on an antidepressant drug for at least 180 days	44	41
Follow-up after hospitalization for mental illness		
4. 7 Days—the percentage of members age 6 and over who had an ambulatory or day/night visit with a mental health practitioner within 7 days of hospital discharge	58	41
5. 30 Days—the percentage of members age 6 and over who had an ambulatory or day/night visit with a mental health practitioner within 30 days of hospital discharge	73	64
Comprehensive diabetes care		
6. HbA1c testing—the percentage of members with diabetes (Type 1 and Type 2) between 18 and 75 who had their Hemoglobin A1c tested	82	77

Description	Average All Plans	This Plan
7. Eye exam—the percentage of members with diabetes (Type 1 and Type 2) between 18 and 75 who had an eye exam for diabetic retinal disease	55	50
8. LDL-C screening—the percentage of members with diabetes (Type 1 and Type 2) between 18 and 75 who had an LDL-C screening	82	77
Prenatal and postpartum care		
9. Timeliness—the percentage of women who received a prenatal care visit in the first trimester	86	92
10. Postpartum care—the percentage of women who had a postpartum visit on or between 21 days and 56 days after delivery	77	78
Beta blocker treatment		
11. The percentage of members 35 or older who were hospitalized with a diagnosis of acute myocardial infarction and who received an ambulatory prescription for beta blockers upon discharge	93	90
Breast cancer screening		
12. The percentage of women age 52 through 69 who had a mammogram during the year	76	73
Cervical cancer screening		
13. The percentage of women age 21 through 64 who received one or more Pap tests during the year	80	76
Cholesterol management after acute cardiovascular events		
14. The percentage of members 18 through 75 who were discharged for acute myocardial infarction, coronary artery bypass graft, or percutaneous transluminal coronary angioplasty and had evidence of LDL-C screening	76	74
Childhood immunization status		
15. DTP—the percentage of children who had four DTP (diphtheria, tetanus, and pertussis) before the age of 2	82	81
16. OPV—the percentage of children who had three OPV (oral polio vaccine) before the age of 2	86	87
17. MMR—the percentage of children who had one MMR (measles, mumps, and rubella) before the age of 2	90	93
18. HiB—the percentage of children who had two HiB (H influenza type b) before the age of 2	84	85
19. Hepatitis B—the percentage of children who had three Hepatitis B before the age of 2	80	86
20. VZV—the percentage of children who had one VZV (chicken pox vaccine) before the age of 2	76	83

Source: Office of Personnel Management, 2002.

FIGURE 1.10 TWO CMS DATA CHARTS.

Source: Centers for Medicare and Medicaid Services, 2002a.

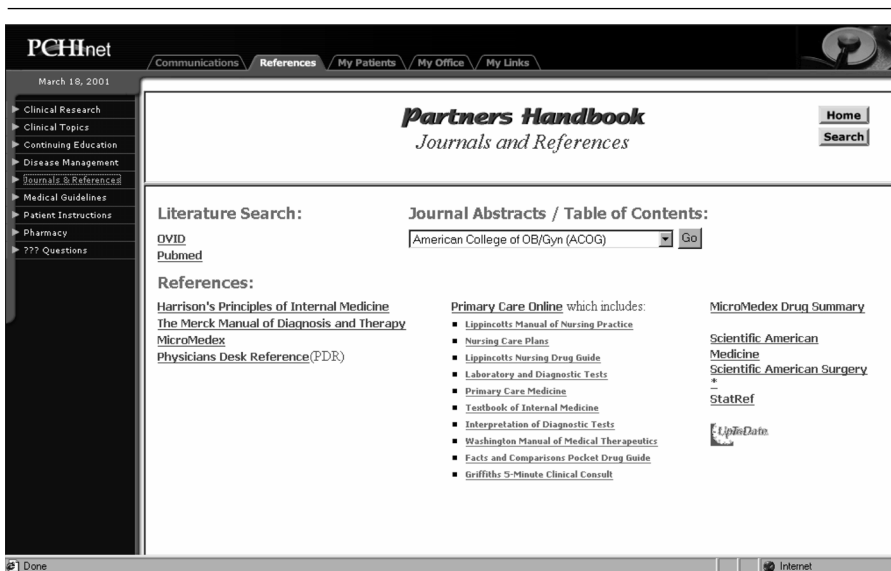
Leapfrog Group. Figure 1.9 (displayed earlier), which lists common data sets, is by no means an exhaustive list of all data sets that could be used by health care organizations for performance comparisons. *Many* other public and private organizations provide this type of data. One that has received a lot of attention in recent times is the Leapfrog Group (2004), which is composed of representatives from more than 150 public and private organizations that provide health care benefits to employees. The Leapfrog Group works to improve patient safety by working with medical experts throughout the United States to identify problems and propose solutions for hospital systems. As one of its activities, the Leapfrog Group collects data from hospitals (who supply this information to Leapfrog on a voluntary basis). These data are reported in a variety of mechanisms. HealthGrades (2004), a technology partner of Leapfrog, publishes *report cards* for the participating hospitals, along with data it has collected on physicians and nursing homes. These report cards are readily available to consumers and others on the HealthGrades Web site (www.healthgrades.com). Other (commercial) sites that use Leapfrog survey data, along with other data, are HealthCarePrice, Select Quality Care, and Sublimo.

Expert or Knowledge-Based Information

JCAHO (2004a) defines knowledge-based information as, “A collection of stored facts, models, and information that can be used for designing and redesigning processes and for problem solving. In the context of the JCAHO accreditation manual, knowledge-based information is found in the clinical, scientific, and management literature.” Health care executives and health care providers rely on knowledge-based information to maintain their professional competence and to discover the latest techniques and procedures. The content of any professional journal would fall into the category of knowledge-based information. Other providers of knowledge-based information are the many on-line health care and health care management references and resources. With the development of rule-based computer systems, the Internet, and *push* technologies, health care executives and providers are finding that they often have access to vast quantities of expert or knowledge-based information at the time they need it, even at the patient bedside. Most clinical and administrative professional organizations not only publish print journals but also maintain up-to-date Web sites where members or other subscribers can get knowledge-based information. Several organizations also provide daily, weekly, or other periodic e-mail notifications of important events that are *pushed* onto subscribers’ personal computers.

Knowledge-based information can also be incorporated into electronic medical records or health care organization Web sites. Figure 1.11 is a sample of the knowledge-based information resources available through an electronic medical record interface.

FIGURE 1.11. SAMPLE ELECTRONIC KNOWLEDGE-BASED INFORMATION RESOURCES.



Source: Partners HealthCare System, Inc.

Summary

Without health care data and information there would be no need for health care information systems. Health care information is a valuable asset in health care organizations and it must be managed like other assets. To manage information effectively, health care executives should have an understanding of the sources and uses of health care data and information. In this chapter we introduced a framework for discussing types of health care information, looked at a wide range of internal data and information whose creation and use must be managed in health care organizations, and also discussed a few associated processes that are typically part of patient encounters. We examined not only patient-specific (individual) internal information

but also aggregate information. We addressed both clinical and administrative data and information in our discussions. In addition we examined several types of external data and information that are available for use by health care organizations, including comparative and knowledge-based data and information. Throughout, our view of data and information was organizational and the focus was on that information that is unique to health care.

Chapter One: Learning Activities

1. Contact a health care facility (hospital, nursing home, physician's office, or other organization) to ask permission to view a sample of the health records they maintain. These records may be in paper or electronic form. Answer the following questions for each record:
 - a. What is the primary reason (or condition) for which the patient was admitted to the hospital?
 - b. How long has the patient had this condition?
 - c. Did the patient have surgery during this admission? If so, what procedure(s) was done?
 - d. Did the patient experience any complications during this admission? If so, what were they?
 - e. How does the physician's initial assessment of the patient compare with the nurse's initial assessment? Where in the record would you find this information?
 - f. To where was the patient discharged?
 - g. What were the patient's discharge orders or instructions? Where in the record should you find this information?
2. Make an appointment to meet with the business manager at a physician's office or health care clinic. Discuss the importance of ICD-9-CM coding or CPT coding (or both) for that office. Ask to view the books or encoders that the office uses to assign diagnostic and procedure codes. After the visit, write a brief summary of your findings and impressions.
3. Visit www.oig.hhs.gov. What are the major responsibilities of the Office of Inspector General as they relate to coded health care data? What other responsibilities related to health care fraud and abuse does this office have?

4. List and briefly describe several types of aggregate health care reports that you believe would be commonly used by health care executives in a hospital or other health care setting.
5. Using the Internet sites identified in this chapter or found during your own searches, find a *report card* for one or more local hospitals. If you were trying to make a decision about which hospital to use for your personal health care or that of a family member, would you find this information useful? Why or why not?



CHAPTER TWO

HEALTH CARE DATA QUALITY

Chapter One provided an overview of the various types of health care data and information that are generated and used by health care organizations. We established the importance of understanding health care data and information in order to reach the goal of having effective health care information systems. There is another fundamental aspect of health care data and information that is also central to developing effective health care information systems—data quality. Consider for a moment an organization with sophisticated health care information systems that affect every type of health care information, from patient specific to knowledge based. What if the quality of the documentation going into the systems is poor? What if there is no assurance that the reports generated from the systems are accurate or timely? How would the users of the systems react? Are those information systems beneficial or detrimental to the organization in achieving its goals?

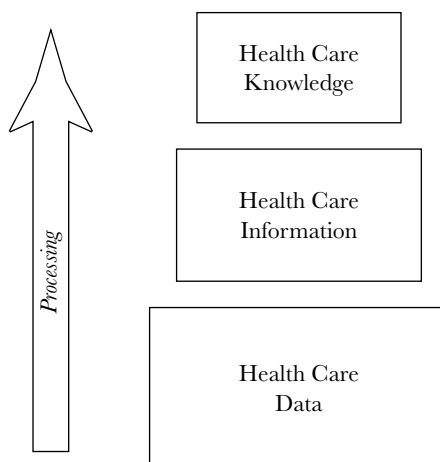
In this chapter we will examine several aspects of data quality. We begin by distinguishing between health care data and health care information. We then look at some problems associated with poor-quality health care data, both at an organizational level and across organizations. The discussion continues with a presentation of two sets of guidelines that can be used in evaluating data quality and ends with a discussion of the major types of health care data errors.

Data Versus Information

What is the difference between data and information? The simple answer is that *information* is *processed data*. Therefore we can say that *health care information* is *processed health care data*. (We interpret *processing* broadly to cover everything from formal analysis to explanations supplied by the individual decision maker's brain.) Health care data are raw health care facts, generally stored as characters, words, symbols, measurements, or statistics. One thing that is apparent about health care data is that they are generally not very useful for decision making. Health care data may describe a particular event, but alone and *unprocessed* they are not particularly helpful. Take for example this figure: 79 percent. By itself, what does it mean? If we process this datum further by indicating that it represents the average bed occupancy for a hospital for the month of January, it takes on more meaning. With the additional facts attached, is this figure now information? That depends. If all a health care executive wants or needs to know is the bed occupancy rate for January, this could be considered information. However, for the hospital executive who is interested in knowing the trend of the bed occupancy rate over time or how the facility's bed occupancy rate compares to that of other, similar facilities, this is not yet information.

Knowledge is seen by some as the highest level in a hierarchy with data at the bottom and information in the middle (Figure 2.1). *Knowledge* is defined by Johns (1997) as "a combination of rules, relationships, ideas, and experience." Another way of thinking about knowledge is that it is information applied to rules, experiences, and relationships, with the result that it can be used for decision making. A journal article that describes the use of bed occupancy rates in decision making or one health care facility's experience with improving its occupancy rates might be an example of knowledge.

Where do *health care data* end and where does *health care information* begin? Information is an *extremely* valuable asset at *all* levels of the health care organization. Health care executives, clinical staff, and others rely on information to get their jobs accomplished. An interesting point to think about is that the same data may provide different information to different users. One person's data may be another person's information. Think back to our bed occupancy example. The health care executive needing verification of the rate for January has found her information. The health care executive needing trend analysis that includes this rate has not. In the second case the rate for January is data needing to be processed further. The goal of this discussion is not to pinpoint where data end and information begins but rather to further an understanding of the relationship between health care data and information—health care data are the beginnings of health care information. You cannot create information without data (Lee, 2002).

FIGURE 2.1. FROM DATA TO KNOWLEDGE.

Problems Associated with Poor-Quality Data

Now that we have established the relationship between health care data and health care information, we can look at some of the problems associated with having poor-quality data. Health care data are the source of health care information, so it stands to reason that a health care organization cannot have high-quality health care information without first establishing that it has high-quality health care data. Data quality must be established at the most *granular* level. Much health care information is gathered through patient care documentation by clinical providers and administrative staff. As was discussed in Chapter One, the patient record is the source for most of the clinical information generated by the health care organization. This clinical information is in turn coded for purposes of reimbursement and research. We also saw that medical record information is shared across many providers and payers, aggregated, and used to make comparisons relevant to health care and related issues.

Poor-quality data collection and reporting can affect each of the purposes for which we maintain patient records. At the organizational level, a health care organization may find diminished quality in patient care, poor communication among providers and patients, problems with documentation, reduced revenue generation due to problems with reimbursement, and a diminished capacity to effectively evaluate outcomes or participate in research activities. Sharon Schott (2003) has summarized some of the common problems associated with poor-quality medical record documentation. She

focuses on the medical record used as evidence in court, but the same documentation problems can lead to poor quality of care, poor communication, and poor documentation. As we will see in later chapters, some of the problems presented may be reduced with the implementation of effective electronic medical record systems.

Perspective: Documentation

In pointing out the serious consequences of documentation problems when records (especially paper-based records) are called into evidence in court cases, Sharon Schott cites several specific examples, including these three:

Simple things such as misspelled names of common drugs or procedures can have a major effect on jurors' impression of the competency of the clinician documenting in the record. In one recent case, a nurse administered 5,000 units of Heparin when the order was for 2,500 units. The patient became critically ill as a result. When the documentation was reviewed, it was discovered that the nurse committing the error had misspelled Heparin as "Hepirin." This spelling error was presented to the jury as an additional demonstration of incompetence. The plaintiff's attorney argued that Heparin is a commonly used drug and obviously this nurse had no knowledge of it, because she couldn't spell it correctly. Juries will also doubt the competence of a nurse who writes "The wound on the left heal is healed."

The nurse who documented an assessment with a post date was called as a witness. She was asked to explain how she could perform an assessment two days after the patient died. The nurse explained that Friday was the actual due date for the assessment but because she had some extra time on Tuesday, she decided to do it early and put Friday's date on it to be compliant with the due date. The plaintiff's attorney then asked, "Is that the only place in the chart that you lied?" Then the jury was suspicious of the integrity of the entire medical record and the nurse.

The continuity of the record also needs special scrutiny on a regular basis. Some institutions allow the record to be "split," which means placing the progress notes at the bedside while maintaining the rest of the chart documentation at the nurses' station. To avoid having to go back to the bedside to document, a nurse might take a new progress note sheet, document findings, and then put the page in the chart at the nurses' station. This documentation will not be in proper sequence with the progress notes from the bedside when they are entered into the chart.

As you read these vignettes, think about ways that information systems could assist in preventing these problems.

Schott, 2003

The problems with poor-quality patient care data are not limited to the patient medical record or other data collected and used at the organizational level. In a recent report, the Medical Records Institute (MRI), a professional organization dedicated to the improvement of patient records through technology, has identified five major functions that are negatively affected by poor-quality documentation (MRI, 2004b). These problems are found not only at the organizational level but also across organizations and throughout the overall health care environment.

- *Patient safety* is affected by inadequate information, illegible entries, misinterpretations, and insufficient interoperability.
- *Public safety*, a major component of public health, is diminished by the inability to collect information in a coordinated, timely manner at the provider level in response to epidemics and the threat of terrorism.
- *Continuity of patient care* is adversely affected by the lack of shareable information among patient care providers.
- *Health care economics* are adversely affected, with information capture and report generation costs currently estimated to be well over \$50 billion annually.
- *Clinical research and outcomes analysis* is adversely affected by a lack of uniform information capture that is needed to facilitate the derivation of data from routine patient care documentation [MRI, 2004b, p. 2].

This same report identifies health care documentation as having two parts: *information capture* and *report generation*. Information capture is “the process of recording representations of human thought, perceptions, or actions in documenting patient care, as well as device-generated information that is gathered and/or computed about a patient as part of health care” (MRI, 2004b, p. 2). Some means of information capture in health care organizations are handwriting, speaking, typing, touching a screen or pointing and clicking on words or phrases, videotaping, audio recording, and generating images through X-rays and scans. Report generation “consists of the formatting and/or structuring of captured information. It is the process of analyzing, organizing, and presenting recorded patient information for authentication and inclusion in the patient’s healthcare record” (MRI, 2004b, p. 2). In order to have high-quality documentation resulting in high-quality data both information capture and report generation must be considered.

Ensuring the Quality of Data and Information

The importance of having quality health care information available to providers and health care executives cannot be overstated. Health care decision makers rely on

high-quality information. The issue is not whether quality information is important but rather how it can be achieved. Before an organization can measure the quality of the information it produces and uses, it must establish data standards. That is, data can be identified as high quality only when they conform to a recognized standard. Ensuring this conformance is not as easy as it might seem because, unfortunately, there is no universally recognized set of health care data quality standards in existence today. One reason for this is that the quality of the data needed in any situation is driven by the use to which the data or the information that comes from the data will be put. For example, in a patient care setting the margin of error for critical lab tests must be zero or patient safety is in jeopardy. However, a larger margin of error may be acceptable in census counts or discharge statistics. Health care organizations must establish data quality standards specific to the intended use of the data or resulting information.

Although we have no nationally recognized data quality standards, two organizations have published guidance that can assist a health care organization in establishing its own data quality standards: the Medical Records Institute (MRI) has published a set of “essential principles of healthcare documentation,” and the American Health Information Management Association (AHIMA) has published a data quality management tool. These two guides are summarized in the following sections.

The MRI Principles of Health Care Documentation

The MRI argues that there are many steps that must be taken to create systems that ensure quality health care documentation. It has developed the following key principles that should be adhered to as these systems (and their accompanying policies) are established:

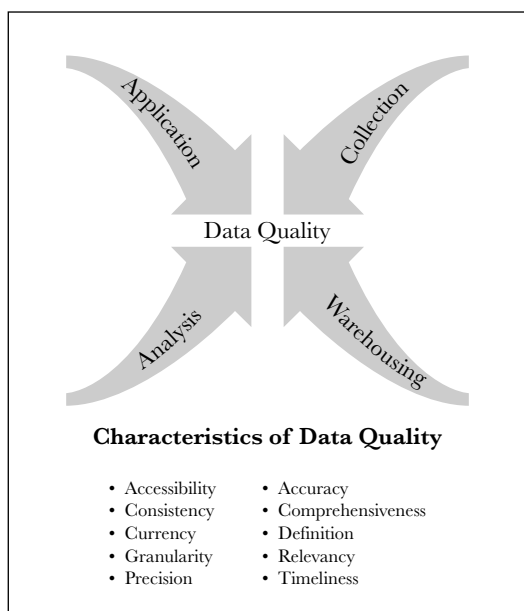
- Unique patient identification must be assured within and across healthcare documentation systems.
- Healthcare documentation must be
 - Accurate and consistent.
 - Complete.
 - Timely.
 - Interoperable across types of documentation systems.
 - Accessible at any time and at any place where patient care is needed.
 - Auditable.
- Confidential and secure authentication and accountability must be provided [MRI, 2004b, p. 3].

The MRI takes the position that when practitioners interact with electronic resources they have an increased ability to meet these guidelines (MRI, 2004b).

The AHIMA Data Quality Model

AHIMA has published a generic data quality management model and an accompanying set of general data characteristics. There are similarities between these characteristics and the MRI principles. AHIMA strives to include all health care data, however, and does limit the characteristics to clinical documentation. The AHIMA model is reprinted in Figure 2.2 and Table 2.1.

FIGURE 2.2. AHIMA DATA QUALITY MANAGEMENT MODEL.



Application – The purpose for which the data are collected.

Collection – The processes by which data elements are accumulated.

Warehousing – Processes and systems used to archive data and data journals.

Analysis – The process of translating data into information utilized for an application.

Source: AHIMA, Data Quality Management Task Force, 1998b.

TABLE 2.1. AHIMA DATA QUALITY MANAGEMENT CHARACTERISTICS.

Characteristic	Application	Collection	Warehousing	Analysis
Data accuracy Data are the correct values and are valid.	To facilitate accuracy, determine the application's purpose, the question to be answered, or the aim for collecting the data element.	Ensuring accuracy involves appropriate education and training and timely and appropriate communication of data definitions to those who collect data. For example, data accuracy will help ensure that if a patient's sex is female, it is accurately recorded as female and not male.	To warehouse data, appropriate edits should be in place to ensure accuracy. For example, error reports should be generated for inconsistent values such as a diagnosis inappropriate for age or gender. Exception or error reports should be generated and corrections should be made.	To accurately analyze data, ensure that the algorithms, formulas, and translation systems are correct. For example, ensure that the encoder assigns the correct codes and that the appropriate DRG is assigned for the codes entered. Also, ensure that each record or entry within the database is correct.
Data accessibility Data items should be easily obtainable and legal to collect.	The application and legal, financial, process, and other boundaries determine which data to collect. Ensure that collected data are legal to collect for the application. For example, recording the age and race in medical records may be appropriate. However, it may be illegal to collect this information in human resources departments.	When developing the data collection instrument, explore methods to access needed data and ensure that the best, least costly method is selected. The amount of accessible data may be increased through system interfaces and integration of systems. For example, the best and easiest method to obtain demographic information may be to obtain it from an existing system. Another method may be to assign data collection by the expertise of each team member. For example, the admission staff collects demographic data, the nursing staff collects symptoms, and the HIM [health information management] staff assigns codes. Team members should be assigned accordingly.	Technology and hardware impact accessibility. Establish data ownership and guidelines for who may access data and/or systems. Inventory data to facilitate access.	Access to complete, current data will better ensure accurate analysis. Otherwise results and conclusions may be inaccurate or inappropriate. For example, use of the Medicare case mix index (CMI) alone does not accurately reflect total hospital CMI. Consequently, strategic planning based solely on Medicare CMI may not be appropriate.

Characteristic	Application	Collection	Warehousing	Analysis
Data completeness All required data items are included. Ensure that the entire scope of the data is collected and document intentional limitations.	Clarify how the data will be used and identify end-users to ensure complete data are collected for the application. Include a problem statement and cost-benefit or impact study when collected data are increased. For example, in addition to outcome it may be important to gather data that impact outcomes.	Cost-effective comprehensive data collection may be achieved via interface to or download from other automated systems. Data definition and data precision impact comprehensive data collection (see these characteristics below).	Warehousing includes managing relationships of data owners, data collectors, and data end-users to ensure that all are aware of the available data in the inventory and accessible systems. This also helps to reduce redundant data collection.	Ensure that all pertinent data impacting the application are analyzed in concert.
Data consistency The value of the data should be reliable and the same across applications.	Data are consistent when the value of the data is the same across applications and systems, such as the patient's medical record number. In addition, related data items should agree. For example, data are inconsistent when it is documented that a male patient has had a hysterectomy.	The use of data definitions, extensive training, standardized data collection (procedures, rules, edits, and process), and integrated/interfaced systems facilitate consistency.	Warehousing employs edits or conversion tables to ensure consistency. Coordinate edits and tables with data definition changes or data definition differences across systems. Document edits and tables.	Analyze data under reproducible circumstances by using standard formulas, scientific equations, variance calculations, and other methods. Compare "apples to apples."

TABLE 2.1. (continued)

Characteristic	Application	Collection	Warehousing	Analysis
Data currency The data should be up-to-date. A datum value is up-to-date if it is current for a specific point in time. It is outdated if it was current at some preceding time yet incorrect at a later time.	The appropriateness or value of an application changes over time. For example, traditional quality assurance applications are gradually being replaced by those with the more current application of performance improvement.	Data definitions change or are modified over time. These should be documented so that current and future users know what the data mean. These changes should be communicated in a timely manner to those collecting data and to the end-users.	To ensure current data are available, warehousing involves continually updating systems, tables, and databases. The dates of warehousing events should be documented.	The availability of current data impacts the analysis of data. For example, to study the incidence of diseases or procedures, ICD-9-CM codes may be used. Coding practices or the actual code for a disease or procedure may change over time. This should be taken into consideration when analyzing trends.
Data definition Clear definitions should be provided so that current and future data users will know what the data mean. Each data element should have clear meaning and acceptable values.	The application's purpose, the question to be answered, or the aim for collecting the data element must be clarified to ensure appropriate and complete data definitions.	Clear, concise data definitions facilitate accurate data collection. For example, the definition of patient disposition may be "the patient's anticipated location or status following release or discharge." Acceptable values for this data element should also be defined. The instrument of collection should include data definitions and ensure that data integrity characteristics are managed.	Warehousing includes archiving documentation and data. Consequently, data ownership documentation and definitions should be maintained over time. Inventory maintenance activities (purging, updates, and others), purpose for collecting data, collection policies, information management policies, and data sources should be maintained over time also.	For appropriate analysis, display data needs to reflect the purpose for which the data were collected. This is defined by the application. Appropriate comparisons, relationships, and linkages need to be shown.

Characteristic	Application	Collection	Warehousing	Analysis
Data granularity The attributes and values of data should be defined at the correct level of detail.	A single application may require varying levels of detail or granularity. For example, census statistics may be utilized daily, weekly, or monthly depending upon the application. Census is needed daily to ensure adequate staffing and food service. However, the monthly trend is needed for long-range planning.	Collect data at the appropriate level of detail or granularity. For example, the temperature of 100° may be recorded. The granularity for recording outdoor temperatures is different from recording patient temperatures. If patient Jane Doe's temperature is 100°, does that mean 99.6° or 100.4°? Appropriate granularity for this application dictates that the data need to be recorded to the first decimal point while appropriate granularity for recording outdoor temperatures may not require it.	Warehouse data at the appropriate level of detail or granularity. For example, exception or error reports reflect granularity based on the application. A spike (exception) in the daily census may show little or no impact on the month-to-date or monthly reports.	Appropriate analysis reflects the level of detail or granularity of the data collected. For example, a spike (exception) in the daily census resulting in immediate action to ensure adequate food service and staffing may have had no impact on analysis of the census for long-range planning.
Data precision Data values should be just large enough to support the application or process.	The application's purpose, the question to be answered, or the aim for collecting the data element must be clarified to ensure data precision.	To collect data precise enough for the application, define acceptable values or value ranges for each data item. For example, limit values for gender to male, female, and unknown; or collect information by age ranges.		
Data relevancy The data are meaningful to the performance of the process or application for which they are collected.	The application's purpose, the question to be answered, or the aim for collecting the data element must be clarified to ensure relevant data.	To better ensure relevancy, complete a pilot of the data collection instrument to validate its use. A "parallel" test may also be appropriate, completing the new or revised instrument and the current process simultaneously. Communicate results to those collecting data and to the end-users. Facilitate or negotiate changes as needed across disciplines or users.	Establish appropriate retention schedules to ensure availability of relevant data. Relevancy is defined by the application.	For appropriate analysis, display data to reflect the purpose for which the data were collected. This is defined by the application. Show appropriate comparisons, relationships, and linkages.

TABLE 2.1. (continued)

Characteristic	Application	Collection	Warehousing	Analysis
Data timeliness Timeliness is determined by how the data are being used and their context.	Timeliness is defined by the application. For example, patient census is needed daily to provide sufficient day-to-day operations staffing, such as nursing and food service. However, annual or monthly patient census data are needed for the facility's strategic planning.	Timely data collection is a function of the process and collection instrument.	Warehousing ensures that data are available per information management policy and retention schedules.	Timely data analysis allows for the initiation of action to avoid adverse impacts. For some applications, timely may be seconds. For others, it may be years.

Note: The terms *data dictionary* and *data warehouse* will be discussed in Chapter Eight. Basically, a data dictionary lists the terms used in an organization's systems. A data warehouse is a specific type of database, used primarily for decision support.

Source: AHIMA, Data Quality Management Task Force, 1998b.

The AHIMA data quality characteristics listed in Table 2.1 can serve as the basis for establishing data quality standards because they represent common dimensions of health care data that should always be present, regardless of the use of the data or resulting information. Here's a further review of these common dimensions:

- *Data accuracy.* Data that reflect correct, valid values are accurate. Typographical errors in discharge summaries and misspelled names are examples of inaccurate data.
- *Data accessibility.* Data that are not available to the decision makers needing them are of no use.
- *Data comprehensiveness.* All of the data required for a particular use must be present and available to the user. Even relevant data may not be useful when they are incomplete.
- *Data consistency.* Quality data are consistent. Use of an abbreviation that has two different meanings provides a good example of how lack of consistency can lead to problems. For example, a nurse may use the abbreviation CPR to mean *cardiopulmonary resuscitation* at one time and use it to mean *computer-based patient record* at another time, leading to confusion.
- *Data currency.* Many types of health care data become obsolete after a period of time. A patient's admitting diagnosis is often not the same as the diagnosis recorded upon discharge. If a health care executive needs a report on the diagnoses treated during a particular time frame, which of these two diagnoses should be included?
- *Data definition.* Clear definitions of data elements must be provided so that both current and future data users will understand what the data mean. One way to supply clear data definitions is to use data dictionaries. A case described by A. M. Shakir offers an excellent example of the need for clear data definitions.

Perspective: Data Definitions

In 1991, a large national health maintenance organization (HMO) was planning to create a disease management program for pediatric care. As part of the planning effort, the HMO decided to conduct a survey of its regional sites to determine the utilization pattern for pediatric care. It sent a questionnaire to each of the 12 regional offices asking these two questions:

1. How many pediatric members were enrolled as of year-end 1990?
2. How many pediatric visits took place in 1990?

On the surface, the questions seemed quite simple and appropriate. The HMO would determine the number of pediatric members and the number of pediatric visits

by region. It could then compute pediatric utilization by region—and across the program as a whole. This data would then be used to determine a baseline for development of utilization management programs and would assist in comparative analysis of pediatric utilization across regions.

There was only one problem—the absence of common data definitions. Each of the regions operated somewhat autonomously and interpreted the request for information differently. As a result, the regional offices raised a number of questions and revealed numerous discrepancies in their interpretations of data definitions:

What is a pediatric member?

A dependent member under the age of 18

A dependent member under the age of 21

A dependent child member, regardless of age

A patient under the age of 18

What is a pediatric visit?

A visit by a pediatric member

A visit by a patient under the age of 18

Any visit to the pediatric department

A visit with a pediatrician

Attempts to answer these questions only raised more questions. What is a member? What does it mean to be enrolled? What is a dependent? How is patient/member age calculated? What is a visit? What is a patient and how does one differ from a member? What is a department? What are the department types? What is a pediatrician?

. . . This story shows us how important it is that suppliers and consumers of data agree on data definitions before exchanging information. Had the regions not revealed their assumptions, the discrepancies in their interpretations of the data definitions might never have been recognized, and the organization would have unknowingly compared apples to oranges. In the long term, a business strategy with significant implications would have been based upon invalid information.

Shakir, 1999

- *Data granularity.* Data *granularity* is sometimes referred to as data *atomicity*. That is, individual data elements are “atomic” in the sense that they cannot be further subdivided. For example, a typical patient’s name should generally be stored as three data elements, last name, first name, middle name—“Smith” and “John” and “Allen”—not as a single data element—“John Allen Smith.” Again, granularity is related to the purpose for which the data are collected. Although it is possible to subdivide a person’s birth date into separate fields for the month, the date, and the

year, this is usually not desirable. The birth date is at its lowest practical level of granularity when used as a patient identifier. Values for data should be defined at the correct level for their use.

- *Data precision.* Precision often relates to numerical data. Precision denotes how close to an actual size, weight, or other standard a particular measurement is. Some health care data must be very precise. For example, in figuring a drug dosage it is not all right to round up to the nearest gram when the drug is to be dosed in milligrams.
- *Data relevancy.* Data must be relevant to the purpose for which they are collected. We could collect very accurate, timely data about a patient's color preferences or choice of hairdresser, but is this relevant to the care of the patient?
- *Data timeliness.* Timeliness is a critical dimension in the quality of many types of health care data. For example, critical lab values must be available to the health care provider in a timely manner. Producing accurate results after the patient has been discharged may be of little or no value to the patient's care.

Types and Causes of Data Errors

Failures of data to meet established quality standards are called *data errors*. A data error will have a negative impact on one or more of the characteristics of quality data. For example, if a final diagnosis is coded incorrectly, that datum is no longer accurate. If the same diagnosis is coded in several different ways, those data are not consistent. Both examples represent data errors. Data errors are often discussed in terms of two types of underlying cause, systematic errors and random errors (Table 2.2). Systematic errors are errors that can be attributed to a flaw or discrepancy in adherence to standard operating procedures or systems. The diagnosis coding errors just described would be systematic errors if they resulted from incorrect programming of the encoding software or improper training of the individuals assigning the codes. Systematic health care data errors can also be caused by unclear data definitions or a failure to comply with the established data collection protocols, such as leaving out required information. If the diagnosis coding errors were the result of poor handwriting or transcription errors, they would be considered random errors. Carelessness rather than lack of training leads to random error (Arts, DeKeizer, & Scheffer, 2002).

Preventing, Detecting, and Fixing Data Errors

Both systematic and random errors lead to poor-quality data and information. Both types need to be prevented to the extent possible. Errors that are not preventable need to be detected so that they can be corrected. There are multiple points during data collection and processing where system design can reduce data errors. Arts, DeKeizer,

TABLE 2.2. SOME CAUSES OF POOR HEALTH CARE DATA QUALITY.

Systematic	Random
Unclear data definitions	Illegible handwriting in data source
Unclear data collection guidelines	Typing errors
Poor interface design	Lack of motivation
Programming errors	Frequent personnel turnover
Incomplete data source	Calculation errors (not built into the system)
Unsuitable data format in the source	
Data dictionary is lacking or not available	
Data dictionary is not adhered to	
Guidelines or protocols are not adhered to	
Lack of sufficient data checks	
No system for correcting detected data errors	
No control over adherence to guidelines and data definitions	

Source: Arts, DeKeizer, & Scheffer, 2002, p. 604.

and Scheffer (2002) have published a useful framework for ensuring data quality in a centralized health care database (or *medical registry*, as these authors call it). Although the entire framework is not reproduced in here, several key aspects are outlined in Figure 2.3. This framework illustrates that there are multiple reasons for data errors and multiple approaches to preventing and correcting these errors.

Summary

Without health care data and information there would be no need for health care information systems. Health care information is a valuable asset in health care organizations and it must be managed like other assets. To manage information effectively, health care executives should have an understanding of health care data and information and recognize the importance of ensuring data quality. Health care decisions, both clinical and administrative, are driven by data and information. Data and information are used to provide patient care and to monitor facility performance. It is critical that the data and information be of high quality. After all, the most sophisticated of information systems cannot overcome the inherent problems associated with poor-quality source data and data collection or entry errors. The data characteristics and frameworks presented here can be useful tools in the establishment of mechanisms for ensuring the quality of health care data.

FIGURE 2.3. ACTIVITIES FOR IMPROVING DATA QUALITY.

Data Error Prevention

Compose a minimum set of necessary data items
Define data and data characteristics in a data dictionary
Develop a data collection protocol
Create user friendly data entry forms or interface
Compose data checks
Create a quality assurance plan
Train and motivate users

Data Error Detection

Perform automatic data checks
Perform data quality audits
Review data collection protocols and procedures
Check inter- and intraobserver variability (if appropriate)
Visually inspect completed forms (online or otherwise)
Routinely check completeness of data entry

Actions for Data Quality Improvement

Provide data quality reports to users
Correct inaccurate data and fill in incomplete data detected
Control user correction of data errors
Give feedback of data quality results and recommendations
Resolve identified causes of data errors
Implement identified system changes
Communicate with users

Source: Arts, DeKeizer, & Scheffer, 2002, p. 605.

Chapter Two: Learning Activities

1. Contact a health care facility (hospital, nursing home, physicians' office, or other facility) to ask permission to view a sample of the health records they maintain. These records may be in paper or electronic form. For each record, answer the following questions about data quality:
 - a. How would you assess the quality of the data in the patient's record? Use the MRI's key principles and AHIMA's data characteristics as guides.
 - b. What proportion of the data in the patient's medical record is captured electronically? What information is recorded manually? Do you think the method of capture affects the quality of the information?
 - c. How does the data quality compare with what you expected?

2. Visit a health care organization to explore the ways in which the facility monitors or evaluates data quality.
3. Consider the following scenarios and the questions they raise about data quality. What should an organization do? How does one create an environment that promotes data quality? What are some of the problems associated with having poor-quality data?

Perspective: Data Quality

A late entry is written to supply information that was omitted at the time of the original entry. It should be done only if the person completing it has total recall of the omission. For example, a nurse completed her charting on December 12, 2002, and forgot to note that the physician had talked with the patient. When she returned to work on December 13, she wrote a late entry for the day before and documented the physician visit. The clinician must enter the current date and the documentation must be identified as a late entry including the date of the omission. Additionally, a late entry should be added as soon as possible.

A late entry cannot be used to supplement a record because of a negative clinical outcome that occurs after the original entry. For example, while a patient received an antibiotic for two days, the nurse charted nothing unusual. Yet, on the third day, the patient had an acute episode of shortness of breath and chest pain and died later that same day. At the time of death, documentation revealed that the patient had a dark red rash on his chest.

An investigation into the cause of death was conducted and all the nurses who provided care during the three days were interviewed and asked whether they had seen the rash prior to the patient's death. None of the nurses remembered the rash. However, one nurse wrote a late entry for each of the first two days that the patient was receiving the antibiotic stating that there was no rash on those days. This is an incorrect late entry. Her statement is part of the investigation conducted after the fact and was not an omission from her original entry.

Schott, 2003



CHAPTER THREE

HEALTH CARE INFORMATION REGULATIONS, LAWS, AND STANDARDS

Chapters One and Two focused on the health care information and data that are available, used, and managed by health care organizations. We mentioned that there are external drivers that affect and in some cases dictate the types of health care information that health care organizations maintain and to a certain extent the ways in which those types are maintained. These external forces take the form of laws, rules, and regulations mandated at both the state and federal levels. Voluntary accreditation standards are additional external forces. In this chapter we will examine more closely the most important of these laws, regulations, and standards and the external organizations that promulgate them. We will do this under two main headings.

In the section titled “Accreditation, Licensure, and Certification,” we define these processes and examine some of the missions and general functions of two of the major accrediting organizations in the United States, the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and the National Committee for Quality Assurance (NCQA), and introduce several other accrediting bodies. The focus of these discussions is how the accreditation, licensure, and certification processes affect health care information and, as a consequence, health care information systems.

Then, in the section titled “Legal Aspects of Managing Health Care Information,” we look at state and federal laws that address the use of the patient medical record as a legal document, and current laws and regulations that govern patient privacy and confidentiality. These legal requirements have a significant impact on how patient-specific health care information is maintained and secured in health care information systems.

Accreditation, Licensure, and Certification

Health care organizations, such as hospitals, nursing homes, home health agencies, and the like, must be licensed to operate. If they wish to file Medicare or Medicaid claims they must also be certified, and if they wish to demonstrate excellence they will undergo an accreditation process. What are these processes, and how are they related? If a health care organization is licensed, certified, and accredited how will this affect the health care information that it creates, uses, and maintains? In this section we will examine each of these processes and their impact on the health care organizations. We will also discuss their relationships with one another.

Facility Licensure

Licensure is the process that gives a facility legal approval to operate. As a rule, state governments oversee the licensure of health care facilities, and each state sets its own licensure laws and regulations. All facilities must have a license to operate and it is generally the state department of health or a similar agency that carries out the licensure function. Licensure regulations tend to emphasize areas such as physical plant standards, fire safety, space allocations, and sanitation. They may also contain minimum standards for equipment and personnel. A few states tie licensure to professional standards and quality of care. In their licensure regulations, most states set minimum standards for the content, retention, and authentication of patient medical records. Figure 3.1 is an excerpt from the South Carolina licensure regulations for hospitals. This excerpt governs patient medical record content (with the exception of newborn patient records, which are addressed in a separate section of the regulations). Although each state has its own set of licensure rules, these are fairly typical in scope and content.

An initial license is required before a facility opens its doors, and this license to operate must generally be renewed annually. Some states allow organizations with JCAHO accreditation to forgo a formal licensure survey conducted by the state; others require the state survey regardless of accreditation status. As we will see in the section on accreditation, JCAHO standards are more detailed and generally more stringent than the state licensure regulations. Also, JCAHO standards are updated annually; most licensure rules are not.

Certification

Certification gives a health care organization the authority to participate in the federal Medicare and Medicaid programs. In other words, an organization must be certified to receive CMS reimbursement. Legislation passed in 1972 mandated that hospitals

**FIGURE 3.1. MEDICAL RECORD CONTENT:
EXCERPT FROM SOUTH CAROLINA STANDARDS
FOR LICENSING HOSPITALS AND
INSTITUTIONAL GENERAL INFIRMARIES.**

601.5 Contents:

A. Adequate and complete medical records shall be written for all patients admitted to the hospital and newborns delivered in the hospital. All notes shall be legibly written or typed and signed. Although use of initials in lieu of licensed nurses' signatures is not encouraged, initials will be accepted provided such initials can be readily identified within the medical record. A minimum medical record shall include the following information:

1. Admission Record: An admission record must be prepared for each patient and must contain the following information, when obtainable: Name; address, including county; occupation; age; date of birth; sex; marital status; religion; county of birth; father's name; mother's maiden name; husband's or wife's name; dates of military service; health insurance number; provisional diagnosis; case number; days of care; social security number; the name of the person providing information; name, address and telephone number of person or persons to be notified in the event of emergency; name and address of referring physician; name and address and telephone number of attending physician; date and hour of admission;
2. History and physical within 48 hours after admission;
3. Provisional or working diagnosis;
4. Pre-operative diagnosis;
5. Medical treatment;
6. Complete surgical record, if any, including technique of operation and findings, statement of tissue and organs removed and post-operative diagnosis;
7. Report of anesthesia;
8. Nurses' notes;
9. Progress notes;
10. Gross pathological findings and microscopic;
11. Temperature chart, including pulse and respiration;
12. Medication Administration Record or similar document for recording of medications, treatments and other pertinent data. Nurses shall sign this record after each medication administered or treatment rendered;
13. Final diagnosis and discharge summary;
14. Date and hour of discharge summary;
15. In case of death, cause and autopsy findings, if autopsy is performed;
16. Special examinations, if any, e.g., consultations, clinical laboratory, x-ray and other examinations.

Source: South Carolina Department of Health and Environmental Control, Standards for Licensing Hospitals and Institutional General Infirmarys, Regulation 61-16 § 601.5 (2003).

had to be reviewed and certified in order to participate in the Medicare and Medicaid programs. At that time the Health Care Financing Administration (now the Centers for Medicare and Medicaid Services [CMS]) developed a set of minimum standards known as the Conditions of Participation (CoPs). The federal government is required to inspect facilities to make sure they meet these minimum standards; however, this survey process is generally contracted out to the states to perform. In the case of hospitals, those accredited by JCAHO are *deemed* to have met the federal certification standards. One interesting historical fact is that the original Conditions of Participation were essentially a copy of the then existing JCAHO standards. The JCAHO standards, however, have undergone tremendous change over the past forty years, while the CoPs have not. Figure 3.2 displays the section of the current Medicare and Medicaid Conditions of Participation for Hospitals that governs the content of hospital medical records.

FIGURE 3.2. MEDICAL RECORD CONTENT: EXCERPT FROM THE CONDITIONS OF PARTICIPATION FOR HOSPITALS.

Sec. 482.24 Condition of participation: Medical record services.

- (c) – Standard: Content of record. The medical record must contain information to justify admission and continued hospitalization, support the diagnosis, and describe the patient's progress and response to medications and services.
 - (1) – All entries must be legible and complete, and must be authenticated and dated promptly by the person (identified by name and discipline) who is responsible for ordering, providing, or evaluating the service furnished.
 - (i) – The author of each entry must be identified and must authenticate his or her entry.
 - (ii) – Authentication may include signatures, written initials or computer entry.
 - (2) – All records must document the following, as appropriate:
 - (i) – Evidence of a physical examination, including a health history, performed no more than 7 days prior to admission or within 48 hours after admission.
 - (ii) – Admitting diagnosis.
 - (iii) – Results of all consultative evaluations of the patient and appropriate findings by clinical and other staff involved in the care of the patient.
 - (iv) – Documentation of complications, hospital acquired infections, and unfavorable reactions to drugs and anesthesia.
 - (v) – Properly executed informed consent forms for procedures and treatments specified by the medical staff, or by Federal or State law if applicable, to require written patient consent.
 - (vi) – All practitioners' orders, nursing notes, reports of treatment, medication records, radiology, and laboratory reports, and vital signs and other information necessary to monitor the patient's condition.
 - (vii) – Discharge summary with outcome of hospitalization, disposition of case, and provisions for follow-up care.
 - (viii) – Final diagnosis with completion of medical records within 30 days following discharge.
-

Source: Conditions of Participation: Medical Record Services, 42 C.F.R. §§ 482.24c *et seq.* (2004).

Accreditation

Accreditation is an external review process that an organization elects to undergo. The accrediting agency grants recognition to organizations that meet its predetermined performance and outcome standards. The review process and standards are devised and regulated by the accrediting agency. By far the best-known health care accrediting agency in the United States is the Joint Commission on Accreditation of Healthcare Organizations (JCAHO). A few other notable accrediting agencies are the National Committee for Quality Assurance (NCQA), the American Osteopathic Association (AOA), the Commission on Accreditation of Rehabilitation Facilities (CARF), and the Accreditation Association for Ambulatory Health Care (AAAHC).

Although accreditation is voluntary, there are financial and legal incentives for health care organizations to seek accreditation. As we stated earlier, JCAHO or AOA accreditation can lead to *deemed* status for CMS programs, and many states recognize accreditation in lieu of their own licensure surveys. Other benefits for an organization are that accreditation

- Is required for reimbursement from certain payers
- Validates the quality of care within the organizations
- May favorably influence liability insurance premiums
- May enhance access to managed care contracts
- Gives the organization a competitive edge over nonaccredited organizations

Joint Commission on Accreditation of Healthcare Organizations

JCAHO's stated mission is "To continuously improve the safety and quality of care provided to the public through the provision of health care accreditation and related services that support performance improvement in health care organizations" (JCAHO, 2004c).

The Joint Commission on Accreditation of Hospitals was formed as an independent, not-for-profit organization in 1951, as a joint effort of the American College of Surgeons, American College of Physicians, American Medical Association, and American Hospital Association. JCAHO has grown and evolved to set standards for and accredit approximately 85 percent of all general hospitals and 95 percent of those with more than 200 beds. Today JCAHO has accreditation programs not only for hospitals but also for organizations that offer ambulatory care, assisted living, long-term care, behavioral health care, home care, laboratory services, managed care, and office-based surgery.

In order to maintain accreditation a health care organization must undergo an on-site survey by a JCAHO survey team every three years. This survey is conducted

to ensure that the organization continues to meet the established standards. The standards themselves are a result of an ongoing, dynamic process that incorporates the experience and perspectives of health care professionals and others throughout the country. New standards manuals are published annually, and health care organizations are responsible for knowing and incorporating any changes as they occur.

There are six official accreditation decisions that can be made by the JCAHO:

- *Accreditation*: for organizations in full compliance.
- *Provisional accreditation*: for organizations that fail to address all requirements for improvement within 90 days following a survey.
- *Conditional accreditation*: for organizations that are not in substantial compliance with the standards. These organizations must remedy the problem areas and undergo an additional follow-up survey.
- *Preliminary denial of accreditation*: for organizations for which there is justification for denying accreditation. This decision is subject to appeal.
- *Denial of accreditation*: for organizations that fail to meet standards and that have exhausted all appeals.
- *Preliminary accreditation*: for organizations that demonstrate compliance with selected standards under a special early survey option.

In addition JCAHO may place an organization on *accreditation watch*. This designation can be publicly disclosed when a *sentinel event* has occurred and the organization fails to make adequate plans to prevent similar events in the future (JCAHO, 2004c). A sentinel event is one that occurs unexpectedly and either leads to or presents a significant risk of death or serious injury.

One clear JCAHO focus is the quality of care provided in health care facilities. This focus on quality dates back to the early 1900s when the American College of Surgeons began surveying hospitals and established a hospital standardization program.—With the program came the question, How is quality of care measured? One of the early concerns of the standardization program was the lack of documentation in patient records. The early surveyors found that documentation was so poor they had no way to judge the quality of care provided. JCAHO's emphasis on health care information and the documentation of care has continued to the present. For example, as the excerpt from JCAHO's information management standards for hospitals, shown in Figure 3.4, suggests, the content of patient records is greatly influenced, if not determined, by these standards. Health care information and patient records remain a major focus for JCAHO accreditation; 150 of the JCAHO hospital standards are scored on the patient medical record alone (JCAHO, 2004a, 2004c).

JCAHO Information Management Standards

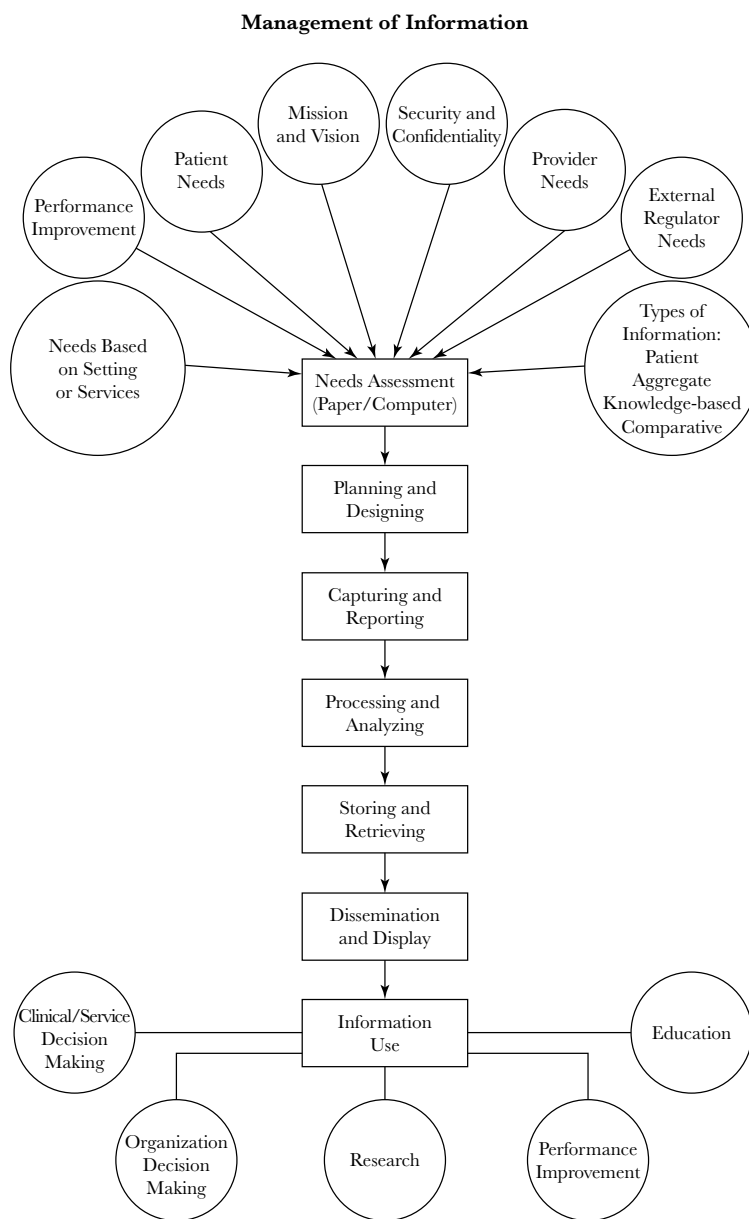
The JCAHO hospital accreditation standards include an entire section devoted to the management of information (IM). These standards were developed under the basic premise that a hospital's provision of care, treatment, and services is "highly dependent on information" and that information is a resource that must be managed like any other resource within a health care facility. The goal of the information management function is "to support decision making to improve patient outcomes, improve health care documentation, assure patient safety, and improve performance in patient care, treatment, and services, governance, management, and support processes" (JCAHO, 2004a). Although JCAHO acknowledges that "efficiency, effectiveness, patient safety, and the quality of patient care, treatment, and services can be improved by computerization and other technologies," the standards apply whether information systems are paper based or electronic. The last section of the IM overview demonstrates JCAHO's strong belief that quality information management influences quality care that continues as we move from paper-based systems to electronic ones: "The quality of care, treatment, and services is affected by the many transitions in information management that are currently in progress in health care, such as the transition from handwriting and traditional paper-based documentation to electronic information management, as well as the transition from free text to structured and interactive text" (JCAHO, 2004a).

Figure 3.3 illustrates the components of the process that hospitals are expected to undertake to be in compliance with the JCAHO IM standards. They must

- Identify their information needs.
- Design the structure of their information management system(s).
- Capture, organize, store, retrieve, process, and analyze data and information.
- Transmit, report, display, integrate, and use data and information.
- Safeguard data and information.

Figure 3.4 presents JCAHO standards for the content and maintenance of patient records. They appear in the Patient Specific Information section of JCAHO's IM standards for hospitals (JCAHO, 2004a). Other sections of these IM standards address

- Information management planning
- Confidentiality and security
- Information management processes
- Information-based decision making

FIGURE 3.3. JCAHO OVERVIEW OF MANAGEMENT OF INFORMATION.

Source: © Joint Commission on Accreditation of Healthcare Organizations: *CAMH: 2004 Comprehensive Accreditation Manual for Hospitals*. Oakbrook Terrace, IL: Joint Commission Resources, 2003. Reprinted with permission.

FIGURE 3.4. JCAHO STANDARDS FOR THE CONTENT AND MAINTENANCE OF PATIENT RECORDS.

Patient-Specific Information

Standard IM.6.10 The hospital has a complete and accurate medical record for every patient assessed or treated.

Elements of Performance for IM.6.10

1. Only authorized individuals make entries in the medical record.
2. The hospital defines which entries made by nonindependent practitioners require countersigning consistent with law and regulation.
3. Standardized formats are used for documenting all care, treatment, and services provided to patients.
4. Every medical record entry is dated, the author identified and, when necessary according to law or regulation and hospital policy, is authenticated.
5. At a minimum, the following are authenticated either by written signature, electronic signature, or computer key or rubber stamp:
 - The history and physical examination
 - Operative report
 - Consultations
 - Discharge summary
6. The medical record contains sufficient information to identify the patient; support the diagnosis/condition; justify the care, treatment, and service; document the course and results of care, treatment, and service; and promote continuity of care among providers.
7. A concise discharge summary providing information to other caregivers and facilitating continuity of care includes the following:
 - The reason for hospitalization
 - Significant findings
 - Procedures performed and care, treatment, and services provided
 - The patient's condition at discharge
 - Instructions to the patient and family, as appropriate
8. The hospital has a policy and procedures on the timely entry of all significant information into the patient's medical record.

FIGURE 3.4. (continued)

9. The hospital defines a complete record and the timeframe within which the record must be completed after discharge, not to exceed 30 days after discharge.
10. The hospital measures medical record delinquency at regular intervals, no less frequently than every three months.

Note: *If the average of the total number of records delinquent (for any reason) calculated from the last four quarterly measurements is equal to or exceeds twice the average monthly discharges, Conditional Accreditation will be recommended. This includes inpatient and outpatient records that are analyzed for completeness.*

11. Medical records are reviewed on an ongoing basis at the point of care and based on organization-defined indicators that address the presence, timeliness, readability (whether handwritten or printed), quality, consistency, clarity, accuracy, completeness, and authentication of data and information contained within the record, as well as appropriate scanning and indexing if document imaging is used.
12. The retention time of medical record information is determined by the hospital based on law and regulation, and on its use for patient care, treatment, and services, legal, research, and operational purposes, as well as educational activities.
13. Original medical records are not released unless the hospital is responding appropriately to federal or state laws, to orders, or subpoenas.
14. Records of patients who have received emergency care, treatment, and services contain the following information:
 - Times and means of arrival
 - Whether the patient left against medical advice
 - The conclusions at termination of treatment, including final disposition, condition, and instructions for follow-up care, treatment, and services
 - Notation that a copy of the record is available to the practitioner or medical organization providing follow-up care, treatment, and services

Standard IM.6.20

Records contain patient-specific information, as appropriate, to the care, treatment, and services provided.

Element of Performance for IM.6.20

1. Each medical record contains, as applicable, the following information:
 - The patient's name, sex, address, date of birth, and authorized representative, if any
 - Legal status of patients receiving behavioral health care services
 - Emergency care, treatment, and services provided to the patient before his or her arrival, if any
 - Documentation and findings of assessments
 - Conclusions or impressions drawn from medical history and physical examination
 - The diagnosis, diagnostic impression, or conditions
 - The reason(s) for admission or care, treatment, and services
 - The goals of the treatment and treatment plan
 - Evidence of known advance directives
 - Evidence of informed consent when required by hospital policy
 - Diagnostic and therapeutic orders
 - All diagnostic and therapeutic procedures, tests, and results
 - Progress notes made by authorized individuals
 - All reassessments and plan of care revisions, when indicated
 - Relevant observations
 - The response to care, treatment, and services provided
 - Consultation reports
 - Allergies to foods and medicines
 - Every medication ordered or prescribed
 - Every dose of medication administered (including the strength, dose, or rate of administration, administration devices used, access site or route, known drug allergies, and any adverse drug reaction)
 - Every medication dispensed or prescribed on discharge
 - All relevant diagnoses/conditions established during the course of care, treatment, and services
 - Records of communication with the patient regarding care, treatment, and services, for example, telephone calls or e-mail, if applicable
 - Patient-generated information (for example, information entered into the record over the Web or in previsit computer systems), if applicable

FIGURE 3.4. (continued)**Standard IM.6.50**

Designated qualified personnel accept and transcribe verbal orders from authorized individuals.

Elements of Performance for IM.6.50

1. Qualified personnel are identified, as defined by hospital policy and, as appropriate, in accordance with state and federal law, and authorized to receive and record verbal orders.
2. Each verbal order is dated and identifies the names of the individuals who gave and received it, and the record indicates who implemented it.
3. When required by state or federal law and regulation, verbal orders are authenticated within the specified time frame.
4. The hospital uses a process for taking verbal or telephone orders or receiving critical test results that requires a verification “read-back” of the complete order or test result by the person receiving the order or test result.

Source: © Joint Commission on Accreditation of Healthcare Organizations: *CAMH: 2004 Comprehensive Accreditation Manual for Hospitals*. Oakbrook Terrace, IL: Joint Commission Resources, 2003. Reprinted with permission.

National Committee for Quality Assurance

The National Committee for Quality Assurance (NCQA) is most closely associated with three activities:

1. The accreditation of managed care organizations (MCOs)
2. The development and implementation of the Health Plan Employer Data and Information Set (HEDIS)
3. Quality Compass

HEDIS and Quality Compass were discussed in Chapter One. In this chapter we will briefly examine the accreditation process for managed care organizations.

NCQA's stated mission and vision are, respectively:

To improve the quality of health care delivered to people everywhere.

To become the most widely trusted source of information driving health care quality improvement [NCQA, 2004].

NCQA began accrediting MCOs in 1991 in response to the need for “standardized, objective information about the quality of these organizations” (NCQA, 2004). Although the NCQA accreditation process is voluntary, three-quarters of all health maintenance organization (HMO) enrollees are in an HMO that has been reviewed by NCQA. Many large employers, including American Airlines, IBM, AT&T, Federal Express, and others, will not do business with a health plan that is not NCQA accredited. More than half of all states recognize NCQA accreditation, eliminating the need for accredited plans to undergo separate state review.

The NCQA accreditation process includes a survey to ensure the organization meets NCQA published standards. There are over sixty specific standards, grouped into five categories:

- *Access and Service*—Do health plan members have access to the care and services they need? Does the health plan resolve grievances quickly and fairly?
 - *Qualified Providers*—Does the health plan thoroughly check the credentials of all of its providers?
 - *Staying Healthy*—Does the health plan help people maintain good health and avoid illness?
 - *Getting Better*—How well does the plan care for members when they become sick?
 - *Living with Illness*—How well does the plan help people manage chronic illness?
- [NCQA, 2004, p. 3].

NCQA accreditation surveys are conducted by teams of physicians and other health care providers. These surveys rely heavily on health care data and information, including the HEDIS measures. The results of the surveys are evaluated by a national oversight committee that assigns one of five accreditation levels:

- Excellent
- Commendable
- Accredited
- Provisional
- Denied

The NCQA accreditation process is viewed as rigorous. A health plan must be aggressively managing quality in order to achieve accreditation at the excellent level. NCQA provides a free, on-line *health plan report card* that shows the accreditation status of all plans that have been surveyed (NCQA, 2004).

Other Accrediting Organizations

Although JCAHO and NCQA are arguably the most visible and well-known accrediting bodies in the U.S. health care system, there are others. The American Osteopathic

Association (AOA) accredits osteopathic health care facilities and laboratories. Like JCAHO, the AOA has been given *deemed authority* by the CMS, meaning that its accreditation may be used in lieu of a CoPs survey process (AOA, 2004). The Commission on Accreditation of Rehabilitation Facilities (CARF) accredits rehabilitative services and programs (CARF, 2004). The Accreditation Association for Ambulatory Health Care (AAAHC) accredits HMOs and ambulatory care organizations (AAAHC, 2003). These accreditation processes have several features in common. They are based on pre-established standards aimed at improving the quality of health care, they require an on-site survey, they make health care information and documentation critical components of the process, and they award a level of accreditation or approval. All have standards that affect organizations' health care information and health care information systems.

In the first half of this chapter, we have taken a brief overview of the accreditation, licensure, and certification processes and of the standards and regulations that affect health care information and information systems. These processes and the standards and regulations provide guidance to organizations for the development of information planning, retention, and retrieval and to a great extent determine the content of patient records. Health care executives must be familiar with the standards, rules, and regulations that apply to their health care organizations to ensure that their information management plans and information systems will facilitate compliance.

Legal Aspects of Managing Health Care Information

Health care information, particularly patient-specific information, is governed by multiple state and federal laws and regulations in addition to those for licensure and certification. Laws and regulations governing the privacy and confidentiality of patient information and also record retention and authentication have existed for many years. When all patient records were on paper, it was fairly easy to identify what constituted a patient record and what did not. Authentication was a signature on a document, and destruction of records involved burning or shredding. As patient records are increasingly stored in electronic form and involve multiple types of media from paper to digital images, implementation of the regulations governing health care information has had to change. In some cases the laws and regulations themselves have been rewritten.

At this juncture it is worth emphasizing that laws governing patient information and medical records vary from state to state and a full discussion of them is beyond the scope of this text. The complexity of the U.S. legal system makes it very important for health care organizations to employ personnel who are knowledgeable about all state and federal laws, rules, and regulations that govern their patients' information

and to have legal counsel available who can provide specific guidance. With that caveat, in this section we will look at several legal aspects of managing health care information, including a brief discussion of some of the significant laws and regulations related to each aspect and a discussion of legal compliance in an increasingly multimedia environment. Specifically, we will address the medical record as a legal document, including the issues of retention and authentication of health care information, and the privacy and confidentiality of patient information, including an overview of HIPAA and the HIPAA Privacy Rule.

The Health Record as a Legal Document

When the patient medical record is a file folder full of paper housed in the health information management department of the hospital, identifying the *legal* record is fairly straightforward. Records kept in the normal course of business (in this case, providing care to patients) represent an exception to the hearsay rule, are generally admissible in a court, and therefore can be subpoenaed—they are legal documentation of the care provided to the patients. The health care organization might struggle with which documents to file in an individual's medical record, because of varying and changing state and federal laws and regulations, but once those decisions are made, the legal record for any given patient could be pulled from the file shelf. Only one “official,” original copy exists.

When the patient record is a hybrid of electronic and paper documents or when it is totally computer based, how does that change the definition of the legal record? There is no simple, one-paragraph answer to this question, as state governments and the federal government are modifying laws and regulations to reflect the change from paper to digital documentation. However, some general guidelines have been proposed (Amatayakul et al., 2001). Figure 3.5 reprints the “Guidelines for Defining the Health Record for Legal Purposes” of the American Health Information Management Association (AHIMA). These guidelines define the *legal health record* (LHR) as “the documentation of the healthcare services provided to an individual in any aspect of healthcare delivery by a healthcare provider organization.” They also recommend that patient-identifiable source data, such as photographs, diagnostic images, tracings, and monitoring strips be considered a part of the LHR. Administrative data and derived data, however, are not considered part of the LHR.

Each health care organization must conduct a thorough review and assessment of how and where patient-identifiable information is stored. Data and information that can be classified as part of the LHR must be identified and included in any resulting LHR definition. The organization should document its definition of the content of the LHR and clearly state in what forms the content originated and is stored.

FIGURE 3.5. AHIMA GUIDELINES FOR DEFINING THE HEALTH RECORD FOR LEGAL PURPOSES.

Legal Health Record

The legal business record generated at or for a healthcare organization. This record would be released upon request.

The LHR is the documentation of the healthcare services provided to an individual in any aspect of healthcare delivery by a healthcare provider organization. The LHR is individually identifiable data, in any medium, collected and directly used in and/or documenting healthcare or health status. The term includes records of care in any health-related setting used by healthcare professionals while providing patient care services, for reviewing patient data, or documenting observations, actions, or instructions. Some types of documentation that comprise the legal health record may physically exist in separate and multiple paper-based or electronic/computer-based databases (see examples listed below).

The LHR *excludes* health records that are *not* official business records of a healthcare provider organization (even though copies of the documentation of the healthcare services provided to an individual by a healthcare provider organization are provided to and shared with the individual). Thus, records such as personal health records (PHRs) that are patient controlled, managed, and populated would not be part of the LHR.

Copies of PHRs that are patient owned, managed, and populated by the individual but are provided to a healthcare provider organization(s) may be considered part of the LHR, if such records are used by healthcare provider organizations to provide patient care services, review patient data, or document observations, actions, or instructions. This includes patient owned, managed, and populated “tracking” records, such as medication tracking records and glucose/insulin tracking records.

Examples of documentation found in the LHR:

- advance directives
- anesthesia records
- care plan
- consent for treatment forms

- consultation reports
- discharge instructions
- discharge summary
- e-mail containing patient-provider or provider-provider communication
- emergency department record
- functional status assessment
- graphic records
- immunization record
- intake/output records
- medication orders
- medication profile
- minimum data sets (MDS, OASIS, etc.)
- multidisciplinary progress notes/documentation
- nursing assessment
- operative and procedure reports
- orders for diagnostic tests and diagnostic study results (e.g., laboratory, radiology, etc.)
- patient-submitted documentation
- pathology reports
- practice guidelines or protocols/clinical pathways that imbed patient data
- problem list
- records of history and physical examination
- respiratory therapy, physical therapy, speech therapy, and occupational therapy records
- selected waveforms for special documentation purposes
- telephone consultations
- telephone orders

FIGURE 3.5. (continued)**Patient-Identifiable Source Data**

An adjunct component of the legal business record as defined by the organization. Often maintained in a separate location or database, these records are provided the same level of confidentiality as the legal business record. The information is usually retrievable upon request. In the absence of documentation (e.g., interpretations, summarization, etc.), the source data should be considered part of the LHR.

Patient-identifiable source data are data from which interpretations, summaries, notes, etc., are derived. Source data should be accorded the same level of confidentiality as the LHR. These data are increasingly captured in multimedia form. For example, in a telehealth encounter, the videotape recording of the encounter would not represent the LHR but rather would be considered source data.

Examples of patient-identifiable source data:

- analog and digital patient photographs for identification purposes only
- audio of dictation
- audio of patient telephone call
- diagnostic films and other diagnostic images from which interpretations are derived
- electrocardiogram tracings from which interpretations are derived
- fetal monitoring strips from which interpretations are derived
- videos of office visits
- videos of procedure
- videos of telemedicine consultations

Administrative Data

While it should be provided the same level of confidentiality as the LHR, administrative data are not considered part of the LHR (such as in response to a subpoena for the “medical record”).

Administrative data are patient-identifiable data used for administrative, regulatory, healthcare operations, and payment (financial) purposes.

Examples of administrative data:

- authorization forms for release of information
- birth and death certificates
- correspondence concerning requests for records
- event history/audit trails
- patient-identifiable claim
- patient-identifiable data reviewed for quality assurance or utilization management
- patient identifiers (e.g., medical record number, biometrics)
- protocols/clinical pathways, practice guidelines, and other knowledge sources that do not imbed patient data

Derived Data

While it should be provided the same level of confidentiality as the LHR, derived data are not considered part of the LHR (such as in response to a subpoena for the “medical record”).

Derived data consists of information aggregated or summarized from patient records so that there are no means to identify patients.

Examples of derived data:

- accreditation reports
- anonymous patient data for research purposes
- best practice guidelines created from aggregate patient data
- MDS report
- OASIS report
- ORYX report
- public health records
- statistical reports

Source: Amatayakul et al., 2001.

Retention of Health Records

The majority of states have specific retention requirements for health care information. These state requirements should be the basis for the health care organization's formal retention policy. (JCAHO and other accrediting agencies also address retention but generally refer organizations back to their own state regulations for specifics.) When no specific retention requirement is made by the state, all patient information that is a part of the LHR should be maintained for at least as long as the state's statute of limitations or other regulation requires. In the case of minor children the LHR should be retained until the child reaches the age of majority as defined by state law, usually eighteen or twenty-one. Health care executives should be aware that statutes of limitations may allow a patient to bring a case as long as ten years after the patient *learns* that his or her care caused an injury (AHIMA, 2002b). In 2002, AHIMA published “recommended retention standards,” which state that patient health records for adults should be retained for ten years after the most recent encounter and patient health records for children should be retained until the time the person reaches the age of majority plus the time stated in the relevant statute of limitations.

Although some specific retention requirements and general guidelines exist, it is becoming increasingly popular for health care organizations to keep all LHR information indefinitely, particularly if the information is stored in an electronic format. If an organization does decide to destroy LHR information, this destruction must be carried out in accordance with all applicable laws and regulations. Some states require that health care organizations create an abstract of the patient record prior to its destruction. Others specify methods of destruction that can be used. If specific methods of destruction are not specified, the health care organization can follow general guidelines,

such as those in the following list (AHIMA, 2002a). These destruction guidelines apply to any patient-identifiable health care information, whether or not that information is identified as part of the LHR.

- Destroy the records so there is no possibility of reconstruction.
 - Burn, shred, pulp, or pulverize paper.
 - Recycle or pulverize microfilm or microfiche.
 - Pulverize write-once read-many laser disks.
 - Degauss computerized data stored on internal or external magnetic media (that is, alter the magnetic alignment of the storage media, making it impossible to recover previously recorded data).
- Document the destruction.
 - Date of destruction.
 - Method of destruction.
 - Description of destroyed records.
 - Inclusive dates of destroyed records.
 - A statement that the records were destroyed in the normal course of business.
 - Signatures of individuals supervising and witnessing the destruction.
- Maintain the destruction documentation indefinitely.

Authentication of Health Record Information

The 2004 JCAHO *Hospital Accreditation Manual* defines authentication as, “The validation of correctness for both the information itself and for the person who is the author or the user of the information” (JCAHO, 2004a). State and federal laws and accreditation standards require that medical record entries be authenticated. This is to ensure that the legal document shows the person or persons responsible for the care provided. Generally, authentication of an LHR entry is accomplished when the physician or other health care professional signs it, either with a handwritten signature or an electronic signature.

Electronic signatures are created when the provider enters a unique code, biometric, or password that verifies his or her identity. Often electronic signatures show up on the computer screen or printout in this form: “Electronically authenticated by Jane H. Doe, M.D.” (AHIMA, 2003b). Electronic signatures are now accepted by both JCAHO and CMS. State laws and regulations vary on the acceptability of electronic signatures, so it is important that health care organizations know what their respective state rules are before implementing such signatures. Most states do allow for electronic signatures in some fashion or are silent on the subject.

Regardless of the state laws and regulations, policies and procedures must be adopted by the health care organization to ensure that providers do not share any codes or passwords that are used to produce electronic signatures. Generally, a provider is required to sign a statement that he or she is the only person who has possession of the signature “key” and that he or she will be the only one to use it (AHIMA, 2003b).

Privacy and Confidentiality

Privacy is an individual’s constitutional right to be left alone, to be free from unwarranted publicity, and to conduct his or her life without its being made public. In the health care environment, *privacy* is the individual’s right to limit access to his or her health care information. *Confidentiality* is the expectation that information shared with a health care provider during the course of treatment will be used only for its intended purpose and not disclosed otherwise. Confidentiality relies on trust.

Recent studies indicate that patients do not fully trust that their private health care information is being kept confidential. Only a third of the adults surveyed in a California HealthCare Foundation national poll (1999) said that they trusted their health plans and government programs to maintain confidentiality all or most of the time. In the same poll, one in six said they had done something out of ordinary to keep medical information confidential. The Health Privacy Project (1999) reports that one in five American adults believes that a health care provider, insurance plan, government agency, or employer has improperly disclosed personal medical information. Half of these individuals also reported that the disclosure resulted in embarrassment or harm. This lack of trust exists in spite of state and federal laws and regulations designed to protect patient privacy and confidentiality and in spite of the ethical tenets under which health care providers work.

There are many sources for the legal and ethical requirement that health care professionals maintain the confidentiality of patient information and protect patient privacy. Ethical and professional standards, such as those published by the American Medical Association and other organizations, address professional conduct and the need to hold patient information in confidence. Accrediting bodies, such as those mentioned in the previous section (JCAHO, NCQA, and so forth), and the CMS CoPs dictate that health care organizations follow standard practice, state, and federal laws to ensure the confidentiality of patient information. State regulations, as a component of state facility licensure or other statutes, also address confidentiality and privacy. However, the regulations and statutes vary widely from state to state. Protections offered by the states also vary according to the holder of the information and the type of information. For example, state regulations may address the confidentiality of AIDS or sexually transmitted disease (STD) information but remain silent on all other types

of health care information. Few states specifically address the redisclosure of information, and the lack of uniformity among states causes difficulty when interstate health care transactions are necessary. In today's environment it is not uncommon for a preferred provider of a technical medical procedure to be out of state. Telemedicine also requires interstate communication of patient information.

In spite of the existing protections, cases of privacy and confidentiality breaches continue to be documented. A few recent violations reported by the Health Privacy Project (2003) are listed in Figure 3.6. Part of the problem is that until recently there was no overarching federal law that outlined privacy rules. Several laws addressed some aspects of keeping patient information confidential, but no single law provided guidance to health care organizations and providers. This lack of a clear federal regulation meant that health information might be released for reasons that had nothing to do with treatment or reimbursement. For example, a health plan could pass information to a lender or employer (*Standards for Privacy* . . . , 2001).

This situation changed with the passage of the Health Insurance Portability and Accountability Act (HIPAA), and more specifically the HIPAA Privacy Rule that was first published in 2000, by the Department of Health of Human Services, and became effective in its current form in 2003. The Privacy Rule establishes a "floor of safeguards"

FIGURE 3.6. RECENT HEALTH CARE PRIVACY VIOLATIONS.

- A North Carolina resident was fired from her job after being diagnosed with a genetic disorder that required treatment (2000).
- The medical records of an Illinois woman were posted on the Internet after she was treated for complications of an abortion (2001).
- An Atlanta truck driver lost his job after his employer was told by the insurance company that the man had sought alcohol abuse treatment (2000).
- A hospital clerk in Florida stole social security numbers from registered patients. These numbers were used to open bank and credit card accounts (2002).
- A computer that contained the files of people with AIDS and other sexually transmitted diseases was put up for sale by the state of Kentucky (2003).
- Due to a software flaw, individuals who had requested drug and alcohol treatment information had their names and addresses exposed through a government run Web site (2001).
- Two health care organizations in Washington state discarded medical records in unlocked dumpsters (2000).

Source: Health Privacy Project, 2003.

to protect confidentiality and privacy. In following sections we will outline the current federal laws and regulations that pertain to privacy and confidentiality, up to and including HIPAA.

Federal Laws Predating HIPAA That Affect Privacy and Confidentiality

In 1966, the Freedom of Information Act (FOIA) was passed. This legislation provides the American public with the right to obtain information from federal agencies. The Act covers all records created by the federal government with nine exceptions. The sixth exception is for personnel and medical information “the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” There was, however, concern that this exception to the FOIA was not strong enough to protect federally created patient records and other health information. Consequently, Congress enacted the Privacy Act of 1974. This Act was written to specifically protect patient confidentiality only in *federally operated* health care facilities, such as Veterans Administration hospitals, Indian Health Service facilities, and military health care organizations. Because the protection is limited to those facilities operated by the federal government, most general hospitals and other nongovernment health care organizations did not have to comply. Nevertheless, the Privacy Act of 1974 was an important piece of legislation, not only because it addressed the FOIA exception for patient information but also because it explicitly stated that patients had a right to access and amend their medical records. It also required facilities to maintain documentation of all disclosures. Neither of these things was standard practice at the time.

During the 1970s, people became increasingly aware of the extra sensitive nature of drug and alcohol treatment records. This led to the regulations currently found in 42 C.F.R. (Code of Federal Regulations) Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records. These regulations have been amended twice, with the latest version published in 1999. They offer specific guidance to health care organizations that treat patients with alcohol or drug problems. Not surprisingly, they set stringent release of information standards, designed to protect the confidentiality of patients seeking alcohol or drug treatment.

HIPAA. The HIPAA Privacy Rule is an important federal regulation. It is the first comprehensive federal rule that offers specific protection to private health information. As we discussed, prior to the HIPAA Privacy Rule, there was no single federal rule governing the privacy and confidentiality of patient-specific information. To put the Privacy Rule in context, we will begin our discussion by briefly outlining the content of the entire Act that authorized this rule. We will then discuss the specifics of the Privacy Rule and its impact on the maintenance, use, and release of health care information.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 has two main parts:

- Title I addresses health care access, portability, and renewability, offering protection for individuals who change jobs or health insurance policies. Although Title I is an important piece of legislation, it does not address health care information specifically and will therefore not be addressed in this chapter.
- Title II includes a section titled Administrative Simplification. It is in a subsection to this section that the requirement to establish privacy regulations for individually identifiable health information is found. Two additional subsections under Administrative Simplification are particularly relevant to health care information: Transaction and Code Sets, standards for which were finalized in 2000, and Security, standards for which were finalized in 2002. (HIPAA security regulations are discussed at length in Chapter Ten.)

HIPAA Privacy Rule. Although the HIPAA Privacy Rule is a comprehensive set of federal standards, it permits the enforcement of existing state laws that are more protective of individual privacy, and states are also free to pass more stringent laws in the future. Therefore health care organizations must still be familiar with their own state rules and regulations related to privacy and confidentiality.

The HIPAA Privacy Rule defines *covered entities*, that is, those individuals and organizations that must comply. This definition is broad and includes

- Health plans, which pay or provide for the cost of medical care.
- Health care clearinghouses, which process health information (for example, billing services).
- Health care providers who conduct certain financial and administrative transactions electronically. (These transactions are defined broadly, so that the reality of the HIPAA Privacy Rule is that it governs nearly all health care providers who receive any type of third-party reimbursement.)

If any of these covered entities shares information with others, it must establish contracts to protect the shared information.

HIPAA-protected information is also defined broadly under the Privacy Rule. *Protected health information (PHI)* is information that

- Relates to a person's physical or mental health, the provision of health care, or the payment for health care
- Identifies the person who is the subject of the information

- Is created *or received* by a covered entity
- Is transmitted or maintained in *any* form (paper, electronic, or oral)

There are five major components to the HIPAA Privacy Rule:

1. *Boundaries.* PHI may be disclosed for health purposes only, with very limited exceptions.
2. *Security.* PHI should not be distributed without patient authorization, unless there is a clear basis for doing so, and the individuals who receive the information must safeguard it.
3. *Consumer control.* Individuals are entitled to access and control their health records and are to be informed of the purposes for which information is being disclosed and used.
4. *Accountability.* Entities that improperly handle PHI can be charged under criminal law and punished and are subject to civil recourse as well.
5. *Public responsibility.* Individual interests must not override national priorities in public health, medical research, preventing health care fraud, and law enforcement in general (CMS, 2002b).

The HIPAA Privacy Rule is fairly new, and as such, it has not been tested by the U.S. legal system. As has occurred with other federal regulations, this rule is likely to undergo some modification or amendment. The tension it sets up inside health care organizations is between the need to *protect* patient information and the need to *use* patient information. Thinking back to Chapter One, remember the purposes for maintaining patient-specific health information. The number one reason is patient care; however, there are other legitimate reasons for sharing or “releasing” identifiable health information.

Release of Information

Because of the various state and federal laws and regulations that exist to protect patient-specific information, health care organizations must have comprehensive release of information policies and procedures in place that ensure compliance. Exhibit 3.1 is a sample of a release of information form used by a hospital, showing the elements that should be present on a valid release form:

- Patient identification (name and date of birth)
- Name of the person or entity to whom the information is being released
- Description of the specific health information authorized for disclosure

EXHIBIT 3.1. SAMPLE RELEASE OF INFORMATION FORM.



AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION	
Patient Name: _____	Date of Birth: _____
Medical Record Number: _____	Social Security Number: _____
I authorize MUSC Medical Center and/or Charleston Memorial Hospital to disclose/release information on the above named individual.	
The type of information to be disclosed is as follows:	
☐ problem list ☐ medication list ☐ laboratory results ☐ physician progress note / visit notes ☐ consultation reports ☐ list of allergies ☐ immunization record ☐ radiology reports ☐ nurses notes ☐ entire record ☐ history and physical ☐ discharge summary ☐ films / images ☐ physician orders ☐ other _____	
For dates of service: _____	
I understand this information may include reference to (check all that apply): ☐ psychiatric/psychological care ☐ drug abuse and/or ☐ sexual assault ☐ results of tests for all infectious diseases including HIV/AIDS. ☐ alcohol abuse and/or	
I authorize the disclosure of this information via (check preferred method): ☐ mail ☐ fax ☐ e-mail ☐ other _____	
The information is to be disclosed to: Name of individual/organization: _____	
Street address: _____ City: _____ State: _____ Zip code: _____	
Phone number: _____ Fax number: _____ E-mail address: _____	
The purpose of the disclosure is: _____	
I understand that I have a right to cancel/revoke this authorization at any time. I understand that if I cancel/revoked this authorization I must do so in writing and present my written cancellation/revocation to the Health Information Services Department (Medical Records). I understand that the cancellation/revocation will not apply to information, which has already been released in response to this authorization as stated in the Notice of Privacy Practice. Unless otherwise canceled/revoked this authorization will expire/end 90 days from this date.	
I understand that a reasonable, cost-based fee for copies of protected health information and postage fees will be charged.	
I understand that authorizing the disclosure of protected health information is voluntary. I can refuse to sign this authorization. I do not need to sign this form to receive treatment. I understand I may review and/or copy the information to be disclosed, as provided in CFR 164.524. I understand that any disclosure of information carries with it the possibility of unauthorized disclosure by the person/organization receiving the information. If I have questions about the disclosure or use of my protected health information, I may contact the MUSC Patient and Family Liaison. The number is (843) 792-5555.	
I understand I will be given a copy of this authorization.	
I understand that if this information is requested in person I will be asked to provide picture identification (e.g. driver's license). A copy of my identification will be made and attached to this authorization.	
Signature of Patient or Legal Guardian/Representative _____	Date _____
Printed Name of Patient or Legal Guardian/Representative _____	
Relationship to Patient, if signed by legal guardian/representative _____	Witness Signature _____
Description of patient representative's authority: _____ (Why patient not signing) To contact Health Information Services (Medical Records) in writing the address is: 169 Ashley Avenue / PO Box 250349 / Attention: Release of Information / Charleston, South Carolina 29425; the phone number is (843) 792-3881.	

Source: © 2004 Medical University Hospital Authority. All Rights Reserved. This form is provided "as is" without any warranty, express or implied, as to its legal effect or completeness. Forms should be used as a guide and modified to meet the laws of your state. Use at your own risk.

- Statement of the reason for or purpose of the disclosure
- Date, event, or condition on which the authorization will expire, unless it is revoked earlier
- Statement that the authorization is subject to revocation by the patient or the patient's legal representative
- Patient's or legal representative's signature
- Signature date, which must be *after the date of the encounter that produced the information to be released*

Health care organizations need clear policies and procedures for releasing patient-identifiable information. There should be a central point of control through which all nonroutine requests for information pass, and all of these disclosures should be well documented.

In some instances patient-specific health care information can be released without the patient's authorization. For example, some state laws require disclosing certain health information. It is always good practice to obtain a patient authorization prior to releasing information when feasible, but in state-mandated cases it is not required. Some examples of situations in which information might need to be disclosed to authorized recipients without the patient's consent are the presence of a communicable disease, such as AIDS and STDs, that must be reported to the state or county department of health; suspected child abuse or adult abuse that must be reported to designated authorities; situations in which there is a legal duty to warn another person of a clear and imminent danger from a patient; bona fide medical emergencies; and the existence of a valid court order.

In addition to situations mandated by law, there are other instances in which patient information can be released without an authorization. In general, health information can be released to another health care provider who is directly involved in the care of the patient, but the rules governing this may vary from state to state. Information can also be released to other authorized persons within a health care organization to facilitate patient care. Information can also be used by the organization for billing or reimbursement purposes once a patient signs a proper consent form for treatment. It may be released for medical research purposes provided all patient identifiers have been removed.

The HIPAA rule attempts to sort out the routine and nonroutine use of health information by distinguishing between patient *consent* to use PHI and patient *authorization* to release PHI. Health care providers and others must obtain a patient's written *consent* prior to disclosure of health information for routine uses of treatment, payment, and health care operations. There are some exceptions to this in emergency situations and the patient has a right to request restrictions on the disclosure. However, health care providers can deny treatment if they feel that limiting the disclosure would be detrimental. Health care providers and others must obtain the patient's written *authorization* for nonroutine uses or disclosures of PHI. This authorization for release of

information has more details than a consent form (see Exhibit 3.1 and the list of necessary elements given earlier), sets an expiration date, and states specifically what, to whom, and for what purpose information is being disclosed (CMS, 2002b).

Summary

In this chapter we examined a number of external drivers that dictate not only the types of health care information that health care organizations maintain but also the way in which they are maintained. These external forces include federal and state laws, rules, and regulations and voluntary accreditation standards. Specifically, this chapter was divided into two main sections. In the first section we defined accreditation, licensure, and certification and examined some of the missions and the general functions of several major accrediting organizations. In the second section we looked at legal issues in managing health care information, including state and federal laws that address the use of the patient medical record as a legal document and current laws and regulations that govern patient privacy and confidentiality. This chapter concluded with discussions of the HIPAA Privacy Rule and release of information practices.

Chapter Three: Learning Activities

1. Visit a health care organization to find out about its current licensure, accreditation, and certification status. How are these processes related to one another in your state?
2. Visit the CMS Web site: www.cms.gov. Find the Conditions of Participation for a particular type of health care facility (hospital, nursing home, and so forth). Review this document and comment on the standards. Are they minimal or optimal standards? Support your answer.
3. Visit the JCAHO Web site: www.jcaho.org. What accreditation programs other than the Hospital Accreditation Program does JCAHO have? List the programs and their respective missions.
4. Visit the NCQA Web site: www.ncqa.org. Look up a health care plan with which you are familiar. What does the report card tell you about this plan?
5. Do an Internet or library search for a recent article discussing the impact of the HIPAA privacy regulations on health care practice. Write a summary of the article.
6. Contact a health care facility (hospital, nursing home, physician's office, or other organization) to talk with the person responsible for maintaining patient records. Ask about the organization's release of information, retention, and destruction policies.



PART TWO

HEALTH CARE INFORMATION SYSTEMS



CHAPTER FOUR

HISTORY AND EVOLUTION OF HEALTH CARE INFORMATION SYSTEMS

After reading Chapters One, Two, and Three (or from your own previous experience), you should have an understanding of the nature of health care information and the processes and regulations that influence the management of information in health care organizations. In this chapter we build upon these fundamental concepts and introduce *health care information systems*, a broad category that includes both administrative and clinical applications. We describe how health care information systems have evolved during the past fifty years. Much of this evolution can be attributed to environmental factors, changes in reimbursement practices, and major advances in information technology. Over the years the health care executive's role and involvement in making information systems-related decisions have also changed considerably. We discuss these changes and conclude by describing the challenges many organizations face as they try to integrate data from various health care applications and to get clinical and administrative applications to interoperate, or “talk,” with each other.

Definition of Terms

Health care executives interact frequently with professionals from a variety of disciplines and may find the terminology used confusing or intimidating. It's no wonder. Most professional disciplines have their own terminology to describe concepts related to their normal course of business. Even professionals within a single discipline often

use different terms to describe the same concepts and the same terms to describe different concepts! Throughout the remainder of this book we will use a variety of terms related to information systems. Our goal is to expose you to many of the information technology–related terms you are likely to encounter in discussions with your organization’s chief information officer, information technology (IT) staff, and IT-savvy health care professionals.

An *information system* (IS) is an arrangement of information (data), processes, people, and information technology that interact to collect, process, store, and provide as output the information needed to support the organization (Whitten, Bentley, & Dittman, 2004). Note that information technology is a component of every information system. *Information technology* is a contemporary term that describes the combination of computer technology (hardware and software) with data and telecommunications technology (data, image, and voice networks). Often in current management literature the terms *information system* and *information technology* are used interchangeably.

In health care the *organization* is the hospital, the physician practice, the integrated delivery system, the nursing home, or the rural health clinic. That is, it is any setting where health-related services are provided. Thus a health care information system (HCIS) is an arrangement of information (data), processes, people, and information technology that interact to collect, process, store, and provide as output the information needed to support the *health care* organization.

This definition is congruent with the definitions provided in Chapter Two. Data are raw facts about people, places, events, and things that are of importance in an organization. Information is data that has been processed or reorganized into a more meaningful form for the user; information can lead to knowledge and facilitate decision making. To simplify, we will assume that the information in a health care information system is made up of both raw and processed data.

There are two primary classes of health care information systems, *administrative* and *clinical*. A simple way to distinguish them is by purpose and the type of data they contain. An *administrative information system* (or an *administrative application*) contains primarily administrative or financial data and is generally used to support the management functions and general operations of the health care organization. For example, an administrative information system might contain information used to manage personnel, finances, materials, supplies, or equipment. It might be a system for human resource management, materials management, patient accounting or billing, or staff scheduling. In contrast a *clinical information system* (or *clinical application*) contains clinical or health-related information used by providers in diagnosing and treating a patient and monitoring that patient’s care. Clinical information systems may be departmental systems such as radiology, pharmacy, or laboratory systems or clinical decision-support, medication administration, computerized provider order entry, or electronic medical record systems, to name a few. They may be limited in their scope to a single area of clinical information (for example, radiology, pharmacy, or laboratory), or they may be

comprehensive and cover virtually all aspects of patient care (as an electronic medical record system does, for example). Clinical information systems will be discussed more fully in Chapter Five. They are presented here in the context of their role in the history and evolution of health care information systems. Table 4.1 lists common types of clinical and administrative health care information systems.

History and Evolution of Health Care Information Systems

The history of the development and implementation of information systems in health care is most meaningful when considered in the context of a chronology of major health care sector and information technology events. In this section we explore the history and evolution of health care information systems in each of the past four decades and in the present era by asking several key questions:

- What was happening in the health care environment and at the federal level that influenced organizations to adopt or use computerized systems?
- What was the state of information technology at the time?
- How did the environmental factors, coupled with advances in information technology, affect the adoption and use of health care information systems?

We start with the 1960s and move forward to the current day (see Table 4.2).

1960s: Billing Is the Center of the Universe; Managing the Money; Mainframes Roam the Planet

It was in the mid-1960s that President Lyndon Johnson signed into law Medicare and Medicaid. These two federal programs provided, for the first time, guaranteed health care insurance benefits to the elderly and the poor. Initially, Medicare provided health care benefits primarily to individuals sixty-five and older. The program has since been expanded to provide health care coverage to individuals with long-term disabilities. Through a combination of federal and state funds, the Medicaid program provides health care coverage to the poor. Initially, both of these programs reimbursed hospitals for services using a cost-based reimbursement methodology. Basically, this meant hospitals were reimbursed for services based on their financial cost reports; in other words, they received a percentage above what they reported it cost them to render the services. Hospitals at the time were also still benefiting from the funds made available through the Hospital Survey and Construction Act (also known as the Hill-Burton Act) of 1946, which had provided them with easier access to capital to build new facilities and expand their services. In these cost-based reimbursement times, the more a hospital built, the more patients it served, and the longer the patients stayed, the more revenue the hospital generated.

**TABLE 4.1. COMMON TYPES OF ADMINISTRATIVE
AND CLINICAL INFORMATION SYSTEMS.**

Administrative Applications	Clinical Applications
Patient administration systems <i>Admission, discharge, transfer (ADT):</i> tracks the patient's movement of care in an inpatient setting <i>Registration:</i> may be coupled with ADT system; includes patient demographic and insurance information as well as date of visit(s), provider information <i>Scheduling:</i> aids in the scheduling of patient visits; includes information on patients, providers, date and time of visit, rooms, equipment, other resources <i>Patient billing or accounts receivable:</i> includes all information needed to submit claims and monitor submission and reimbursement status <i>Utilization management:</i> tracks use and appropriateness of care	Ancillary information systems <i>Laboratory information:</i> supports collection, verification, and reporting of laboratory tests <i>Radiology information:</i> supports digital image generation (picture archiving and communication systems [PACS]), image analysis, image management <i>Pharmacy information:</i> supports medication ordering, dispensing, and inventory control; drug compatibility checks; allergy screening; medication administration Other clinical information systems <i>Nursing documentation:</i> facilitates nursing documentation from assessment to evaluation, patient care decision support (care planning, assessment, flow-sheet charting, patient acuity, patient education) <i>Electronic medical record (EMR):</i> facilitates electronic capture and reporting of patient's health history, problem lists, treatment and outcomes; allows clinicians to document clinical findings, progress notes, and other patient information; provides decision-support tools and reminders and alerts
Financial management systems <i>Accounts payable:</i> monitors debts incurred by the organization and status of purchases <i>General ledger:</i> monitors general financial management and reporting <i>Personnel management:</i> manages human resource information for staff, including salaries, benefits, education, training	<i>Computerized provider order entry (CPOE):</i> enables clinicians to directly enter orders electronically and access decision-support tools and clinical care guidelines and protocols <i>Telemedicine and telehealth:</i> supports remote delivery of care; common features include image capture and transmission, voice and video conferencing, text messaging <i>Rehabilitation service documentation:</i> supports the capturing and reporting of occupational therapy, physical therapy, and speech pathology services

Administrative Applications	Clinical Applications
<i>Materials management:</i> monitors ordering and inventory of supplies, equipment needs and maintenance	<i>Medication administration:</i> typically used by nurses to document medication given, dose, and time
<i>Payroll:</i> manages information about staff salaries, payroll deductions, tax withholding, pay status	
<i>Staff scheduling:</i> assists in scheduling and monitoring staffing needs	
<i>Staff time and attendance:</i> tracks employee work schedules and attendance	

Health care executives realized that to capitalize on these sources of funds, their organizations needed information systems that could automate the patient billing process and facilitate accurate cost reporting. Most of the early information systems in health care were therefore administrative applications almost exclusively driven by financial needs. The primary focus was to collect and process patient demographic data and insurance information and merge it with charge data to produce patient bills. The sooner the hospital could bill Medicare or Medicaid, the sooner it could get paid for services. Patient accounting systems also enabled hospitals to keep better records of all activities, reducing the amounts of *lost charges* and *unbilled services*. Revenue reports and volume of service statistics were needed to justify new capital equipment, just as billing, accounts receivable, and general ledger data were needed for reimbursement. Few clinical data were captured by these information systems.

The administrative applications that existed in the 1960s were generally found in large hospitals, such as those affiliated with academic medical centers. These larger facilities were often the only ones with the resources and staff available to develop, implement, and support such systems. These facilities often developed their own administrative or financial information systems in-house, in what were then known as data processing departments. Reflecting its primary purpose, the data processing department was generally under the direction of the finance department or chief financial officer. The data processing department got its name from the fact that the systems were transaction based, with the primary function of processing billing data.

These early administrative and financial applications ran on large *mainframe* computers (Figure 4.1), which had to be housed in large rooms, with sufficient environmental controls and staff to support them. Because the IS focus at the time was on automating manual administrative processes, only the largest, most complex tasks were candidates for mainframe computing. This limited the development of departmental or clinical systems. The mainframe was also associated with centralized rather than distributed computing. Centralized computing meant that end users entered data

through *dumb* terminals, which were connected to a remote computer, the mainframe, where the data were processed. A dumb terminal had no processing power itself but was simply a device for entering data and viewing results.

Recognizing that small, community-based hospitals could not bear the high cost of an in-house, mainframe system, leading vendors began to offer *shared systems*, so called because they allowed hospitals to share the use of a mainframe with other hospitals. A hospital using a shared system captured billing data manually or electronically and sent them in *batch* form to a company that then processed the claims for the hospital. Most shared systems processed data in a central or regional data center. Shared Medical Systems (now known as Siemens), located in Malvern, Pennsylvania, was one of the first vendors to offer data processing services to hospitals. The vendors charged participating hospitals for computer time and storage, for the number of terminals connected, and for reports. Like many of the in-house systems, most shared systems began with financial and patient accounting functions and gradually migrated toward clinical functions, or applications.

TABLE 4.2. TIMELINE OF MAJOR EVENTS + ADVANCES IN INFORMATION TECHNOLOGY = HCIS.

Decade	Health Care Environment	State of Information Technology	Use of Health Care Information Systems
1960s	-Enactment of Medicare and Medicaid -Cost-based reimbursement -“Building” mode -Focus on financial needs and capturing revenues	-Large mainframe computers -Centralized processing -Few vendor-developed products	-Administrative or financial information systems used primarily in large hospitals and academic medical centers • Developed and maintained in-house • Shared systems available to smaller hospitals -Centralized data processing
1970s	-Still time of growth Medicare and Medicaid expenditures rising -Late in decade, recognition of need to contain health care costs	-Mainframes still in use -Minicomputers become available, smaller, more affordable	-Turnkey systems available through vendor community -Increased interest in clinical applications (for example, laboratory, radiology, pharmacy) -Shared systems still used

Decade	Health Care Environment	State of Information Technology	Use of Health Care Information Systems
1980s	-Medicare introduces prospective payment system for hospitals -Medicaid and private insurers follow suit -Need for financial and clinical information	-Microcomputer or personal computer (PC) becomes available—far more powerful, affordable; brings computing power to desktop; revolutionizes how companies process data and do business -Advent of local area networks	-Distributed data processing -Expansion of clinical information systems in hospitals -Physician practices introduce billing systems -Integrating financial and administrative information becomes important
1990s	-Medicare changes physician reimbursement to RBRVS -Health care reform efforts of Clinton era (HIPAA) -Growth of managed care and integrated delivery systems -IOM calls for computer-based patient record (CPR) adoption	-Unveiling of the Internet and World Wide Web—revolutionizes how organizations communicate with each other, market services, conduct business	-Growth of Internet has profound effect on health care organizations -Vendor community explodes -Products more widely available and affordable -Enterprise-wide systems -Increased interest in clinical application -Relatively small percentage of health care organizations adopt CPR
2000+	-IOM report on patient safety and medical errors -HHS calls for standards for electronic health records (EHRs) -Homeland security -Leapfrog Group -HIPAA regulations -Disparities of care -Spiraling health care costs -High cost of prescription drugs -Possible reimbursement incentives for EHR users	-Internet expansion continues -Emerging technologies become more widespread -Wireless technology -Voice recognition -Bar coding -PDAs	-Focus on electronic health record -HHS gets involved—charges IOM and Health Level Seven (HL7) with developing standards for EHR -Organizations struggle with implementing CPOE, medication administration, and other decision-support systems designed to improve patient care

FIGURE 4.1. TYPICAL MAINFRAME COMPUTER.



Source: Medical University of South Carolina.

1970s: Clinical Departments Wake Up; Debut of the Minicomputer

By the 1970s, health care costs were escalating rapidly, partially due to high Medicare and Medicaid expenditures. Rapid inflation in the economy, expansion of hospital expenses and profits, and changes in medical care, including greater use of technology, medications, and conservative approaches to treatment also contributed to the spiraling health care costs. Health care organizations began to recognize the need for better

access to clinical information for specific departments and for the facility as a whole. Departmental systems began to emerge as a way to improve productivity and capture charges and thereby maximize revenues.

The development of departmental systems coincided with the availability of *mini-computers*. Minicomputers were smaller and also more powerful than some main-frame computers and available at a cost that could be justified by a clinical department such as laboratory or pharmacy. At the same time, improvements in handling clinical data and specimens often showed a direct impact on the quality of patient care because of faster turnaround of tests, more accurate results, and a reduction in the number of repeat procedures (Kennedy, Davis, & Heda, 1992). The increased demand for patient-specific data coupled with the availability of relatively low-cost minicomputers opened a market for a host of new companies that wanted to develop applications for clinical departments, particularly *turnkey systems*. These software systems, which were developed by a vendor and installed on a hospital's computers, were known as *turnkey systems* because all a health care organization had to do was turn the system on and it was fully operational. Rarely could a turnkey system be modified to meet the unique information needs of an organization, however. What you saw was essentially what you got.

As in the 1960s, the health care executive's involvement in information system-related decisions was generally limited to working to secure the funds needed to acquire new information systems, although now executives were working with individual clinical as well as administrative departments on this issue. Most systems were still stand-alone and did not interface well with other administrative or clinical information systems in the organization.

1980s: Computers for the Masses; Age of the Cheap Machine; Arrival of the Computer Utility

Although the use of health care information systems in the 1970s could be considered an extension of the applications used in the 1960s, with a slight increase in the use of clinical applications, the 1980s saw an entirely different story. Sweeping changes in how Medicare reimbursed hospitals and others for services, coupled with the advent of the microcomputer, radically changed how health care information systems were viewed and used. In 1982, Medicare shifted from a cost-based reimbursement system for hospitals to a prospective payment system based on diagnosis related groups (DRGs). This new payment system had a profound effect on hospital billing practices. Reimbursement amounts were now dependent on the patient's diagnosis, and the accuracy of the ICD-9-CM codes used for each patient and his or her subsequent DRG assignment became critical. Hospitals received a predetermined amount based

on the patient's DRG, regardless of the cost to treat that patient. The building and revenue enhancement mode of the 1960s and '70s was no longer always the best strategy for a hospital financially. The incentives were now directed at ordering fewer diagnostic tests, performing fewer therapeutic procedures, and planning for the patient's discharge at the time of admission. Health care executives knew they needed to reduce expenses and maximize reimbursement. Services that had once been available only in hospitals now became more widespread in less resource-intensive outpatient settings and ambulatory surgery centers. As Medicare and many state Medicaid programs began to reimburse hospitals under the DRG-based system, many private insurance plans quickly followed suit.

Hospitals were not the only ones singled out to contain health care costs. Overall health care costs in the 1980s rose by double the rate of inflation. Health insurance companies argued that the traditional *fee-for-service* method of payment to physicians failed to promote cost containment. Managed care plans began to emerge in parts of the nation, and they reimbursed physicians based on *capitated* or fixed rates.

At the same time, as changes were made in reimbursement practices, large corporations began to integrate the organizations making up the hospital system (previously a decentralized industry), enter many other health care-related businesses, and consolidate control. Overall there was a shift toward privatization and corporatization of health care. The integrated delivery system began to emerge, whereby health care organizations offered a spectrum of health care services, from ambulatory care, to acute hospital care, to long-term care and rehabilitation.

With these environmental changes happening in health care, the development of the *microcomputer* in the mid-1980s could not have been more timely. The microcomputer, or personal computer (PC), was smaller, often as or more powerful, and far more affordable than a mainframe computer. Health care information system vendors were developing administrative and clinical applications for a variety of health care settings and touting the possibilities available in bringing "real computing power" to the user at his or her workstation. Health care executives viewed this as an enormous opportunity for health care organizations, particularly hospitals, to acquire and implement needed clinical information systems. Again, the major focus was on revenue-generating departments.

Although most organizations had patient demographic and insurance information available in their administrative applications, rarely were they able to integrate the clinical and the financial information needed to evaluate care and the cost of delivering that care in this new environment. Most of the clinical information systems or applications were being acquired piecemeal. For example, it was not uncommon for the director of laboratory services to go out and purchase from the vendor community the "best" laboratory information system, the pharmacy director to select the "best" pharmacy system, and so forth. This concept of selecting the "best of breed" among vendors and systems became prevalent in the 1980s and still exists to some extent today. Organizations that adopted the best-of-breed approach then faced a

challenge when they tried to build interfaces or integrate data so that the different systems could interoperate, or communicate with each other. System integration remains a primary challenge for many health care organizations. There is no simple solution to getting these disparate systems to talk to each other.

The use of microcomputers was not confined to large hospitals. During this era a computer market opened among home health organizations, small hospital departments, and physician practices. These health care settings had historically lacked the financial and personnel resources to support information systems. The advent of the microcomputer brought computing capabilities to a host of smaller organizations. It also led to users' being more demanding of information systems, asking the information system function to be more responsive.

Sharing information among microcomputers also became possible with the development of local area networks. A *local area network* (LAN) is a group of computers and associated devices that are controlled by a single organization. Usually, one or more *servers* houses applications and data storage that are then shared by multiple PC users. A LAN may serve as few as two or three users (for example, in a home network) or as many as thousands of users (for example, in a large academic medical center). Specific LAN technologies will be discussed in Chapter Eight.

1990s: Health Care Reform Initiatives; Advent of the Internet

The 1990s marked another time of great change in health care. It also marked the evolution and widespread use of the Internet along with a new focus on electronic medical records. In 1992, owing partly to the success of the DRG-based reimbursement system for hospitals, Medicare introduced a new method for reimbursing physicians. Formerly paid under a customary, prevailing, and reasonable rate methodology, physicians treating Medicare patients were now reimbursed for services under the resource-based relative value scale (RBRVS). The RBRVS payment method factored provider time, effort, and degree of clinical decision making into relative value units. RBRVS was initially designed to redistribute funds from specialty providers to primary care providers. That is, the system would reward financially the physicians who spent time educating patients, while discouraging or limiting reimbursement to highly skilled specialists who tended to perform invasive procedures and order an extensive number of diagnostic and therapeutic tests.

Under the RBRVS system, primary care physicians such as family medicine, internal medicine, and pediatric physicians began to see slight increases in reimbursement for their services, and specialty physicians such as ophthalmologists, surgeons, and radiologists experienced decreases in payments. In addition to this new payment scheme for physicians, health care organizations and communities promoted preventive medicine with the goal of promoting health and well-being and preventing disease. Much of preventive medicine and health promotion occurred in the primary

care physician's practice. The emphasis on preventive medicine was the foundation on which the concept of managed care was built. The thought was that if we educate and help keep patients well, the overall cost of providing health care services will be lower in the long run. The primary care provider was viewed as the *gatekeeper* and assumed a pivotal role in the management of the patient's care. Under this managed care model, physicians were reimbursed on a capitated or fixed rate (for example, per member per month) or some type of discounted rate (for example, preferred provider).

The changes in physician reimbursement and the increased focus on prevention guidelines and disease management in the 1990s had implications for the community-based physician practice and its use of information systems. Up until this time, most of the major information systems development had occurred in hospitals. Some administrative information systems were used in physician practices for billing purposes, but as physician payment relied increasingly on documentation substantiated in the patient's record and as computers became more affordable, physicians began to recognize the need for timely, accurate, and complete financial *and* clinical information. Early adopters of clinical information systems also found electronic prompts and preventive health reminders helpful in managing patient care more effectively and efficiently. Likewise, more vendor products designed specifically with the physician practice setting in mind were becoming available.

Health plans, particularly those with a managed care focus, began encouraging health care providers to manage patients' care differently, particularly patients with chronic diseases. Practice guidelines and standards of care were developed and made available to physicians to use in caring for these patients. Subsequently, several vendors developed electronic *disease management programs* that facilitated the management of chronic diseases and were incorporated into clinical applications. Patients could assume a more active role in monitoring their own care. For example, clinicians at Brigham and Women's Hospital introduced a disease management program called Matrix that enables providers to plan, deliver, monitor, and improve the quality and outcomes of the treatment and care delivered to patients with diabetes. This program gives clinicians the tools to automate the planning and delivery of patient care as well as monitor and analyze clinical results on an ongoing basis. Disease management programs have also been shown to be effective in helping providers and patients manage mental health issues and conditions such as hypertension, asthma, and unstable angina (Raymond & Dold, 2002).

In 1991, the Institute of Medicine (IOM) published its landmark report *Computer-Based Patient Records: An Essential Technology for Health Care*. This report brought international attention to the numerous problems inherent in paper-based medical records and called for the adoption of the computer-based patient record (CPR) as the standard by the year 2001. The IOM defined the CPR as "an electronic patient record that resides in a system specifically designed to support users by providing accessibility

to complete and accurate data, alerts, reminders, clinical decision support systems, links to medical knowledge, and other aids” (IOM, 1991, p. 11). This vision of a patient’s record offered far more than an electronic version of existing paper records—the IOM report viewed the CPR as a tool to assist the clinician in caring for the patient by providing him or her with reminders, alerts, clinical decision support capabilities, and access to the latest research findings on a particular diagnosis or treatment modality. We will discuss the status of CPR systems and related concepts (for example, the electronic medical record and the electronic health record) in the next chapter. At this point in the history and evolution of health care information systems, it is important to understand the IOM report’s impact on the vendor community and health care organizations. Leading vendors and health care organizations saw this report as an impetus toward radically changing the ways in which patient information is managed and patient care is delivered. During the 1990s, a number of vendors developed CPR systems. Yet only 10 percent of hospitals and less than 15 percent of physician practices had implemented them by the end of the decade (Goldsmith, 2003). These percentages are particularly low when one considers the fact that by the late 1990s, CPR systems had reached the stage of reliability and technical maturity needed for widespread adoption in health care.

Five years after the IOM report advocating computer-based patient records was published, President Clinton signed into law the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA was designed to make health insurance more affordable and accessible, but it also included important provisions to simplify administrative processes and to protect the confidentiality of personal health information. All of these initiatives were part of a larger health care reform effort and a federal interest in health care IT for purposes beyond reimbursement. Before HIPAA, it was not uncommon for health care organizations and health plans to use an array of systems to process and track patient bills and other information. Health care organizations provided services to patients with many different types of health insurance and had to spend considerable time and resources to make sure each claim contained the proper format, codes, and other details required by the insurer. Likewise, health plans spent time and resources to ensure their systems could handle transactions from a host of different health care organizations, providers, and clearinghouses. The adoption of electronic transaction and code set standards and the greater use of standardized electronic transactions is expected to produce a net savings to the health care sector of nearly \$30 billion over ten years, according to Department of Health and Human Services estimates (65 Fed. Reg. 160, 50312–50372, August 17, 2000). In addition, the administrative simplification provisions led to the establishment of health privacy and security standards. Even though it is too early to tell the full impact of HIPAA legislation on the health care sector, one thing is certain: HIPAA is on the agenda of health care executives and has required a substantial investment of resources by health care organizations.

HIPAA also brought national attention to the issues surrounding the use of personal health information in electronic form. During the first half of the 1990s, microcomputers had become smaller, less expensive, and were to be found not only in the workplace but in the homes of middle-class America. The Internet, historically used primarily by the U.S. Department of Defense and academic researchers, was now widely available, through the World Wide Web, to consumers, businesses, and virtually anyone with a microcomputer and a modem. Health care organizations, providers, and patients could connect to the Internet and have access to a worldwide library of resources—and at times to patient-specific health information. In the early years of its use in health care, many health care organizations and vendors used the Internet to market their services, provide health information resources to consumers, and give clinicians access to the latest research and treatment findings. Other health care organizations saw Internet use as a strategy for changing how, where, and when they delivered health care services. The overall effects of Internet resources and capabilities on health care may not be fully realized for decades to come. We do know, however, that the Internet has provided affordable and nearly universal connectivity, enabling health care organizations, providers, and patients to connect to each other and the rest of the health care system. Along with the microcomputer, the Internet is perhaps the single greatest technological advancement in this era. It revolutionized the way that consumers, providers, and health care organizations access health information, communicate with each other, and conduct business. Health futurist Jeff Goldsmith (2003) describes the Internet as “a technology enabler or, in military jargon, a force multiplier, that helps lower communications and transaction cost, time and complexity. It is also a lubricant of information flow and a solvent of organization boundaries. It may take at least another decade before the health system realizes the full extent of its transformative potential” (pp. 30–31).

With the advent of the Internet and the availability of microcomputers, came *electronic mail* (e-mail). Consumers began to use e-mail to communicate with colleagues, businesses, family, and friends. It substantially reduced or eliminated needs for telephone calls and regular mail. E-mail is fast, easy to use, and fairly widespread. Consumers soon discovered that they could not only search the Internet for the latest information on a particular condition but could then also e-mail that information or questions to their physicians. In a 2000 survey (Baker, Wagner, Singer, & Bundorf, 2003) of e-mail users, although only 6 percent of participants reported sending an e-mail message to their physician, more than half wished to do so. MacDonald (2003) and others (Moyer, Stern, Dobias, Cox, & Katz, 2002) have found that many patients are beginning to use e-mail and other on-line communications and are dragging their physicians along.

The use of *telemedicine* and *telehealth* has also become more prevalent during the past few decades, particularly during the 1990s with its major advancements in telecommunications. Telemedicine is the use of telecommunications for the clinical

care of patients and may involve various types of electronic delivery mechanisms. It is a tool that enables providers to deliver health care services to patients at distant locations. Most telemedicine programs have been pilot programs or demonstration projects that have not endured beyond the life of specific research and development funding initiatives. Reimbursement policies for these services vary, and that has been a significant limiting factor. In 2003, federal legislation allowed health care organizations to be reimbursed for professional consultations via telecommunication systems with specific clinicians when patients are seen at qualifying sites. State reimbursement policies for telemedicine for Medicaid patients vary from state to state. And local third-party payers have individual practices for reimbursing for telemedicine services (American Telemedicine Association, 2003). Until reimbursement issues are addressed at the federal, state, and local levels, the future of telemedicine and telehealth is uncertain.

2000 to Today: Health Care IT Arrives; Patients Take Center Stage

It may be too early to predict how health care organizations will use information technology in the present decade, but if the past is any indication, health care executives should continue to pay close attention to major health care concerns or issues, evaluate proposed changes in reimbursement structures, and keep a finger on the pulse of advances in information technology. At the time of this writing, a number of pressing issues are facing health care organizations, one of which is patient safety and medical errors. In 2000, the IOM published *To Err Is Human: Building a Safer Health Care System*, a report that brought national attention to the fact that an estimated 98,000 patients die each year due to medical errors. In 2004, the IOM Committee on Data Standards for Patient Safety published *Patient Safety: Achieving a New Standard for Care*, a report calling for health care organizations to adopt information technology capable of collecting and sharing essential health information on patients and their care. The IOM committee examined the status of current standards, including standards for health data interchange, terminologies, and medical knowledge representation. Here is an example of the committee's conclusions:

Perspective: The IOM on Patient Safety

As concerns about patient safety have grown, the health care sector has looked to other industries that have confronted similar challenges, in particular, to the airline industry. This industry learned long ago that information and clear communications are critical to the safe navigation of an airplane. To perform their jobs well and guide their plane safely to its destination, pilots must communicate with the airport controller concerning their destination and current circumstances (e.g., mechanical or other problems), their flight plan, and environmental factors (e.g., weather conditions) that could necessitate a change in course. Information must also pass seamlessly from one controller

to another to ensure a safe and smooth journey for planes flying long distances; provide notification of airport delays or closures due to weather conditions; and enable rapid alert and response to extenuating circumstance, such as a terrorist attack.

Information is as critical to the provision of safe health care—care that is free of errors of both commission and omission—as it is to the safe operation of aircraft. To develop a treatment plan, a doctor must have access to complete patient information (e.g., diagnoses, medications, current test results, and available social supports) and to the most current science base.

IOM, Committee on Data Standards for Patient Safety, 2004

Whereas *To Err Is Human* focused primarily on errors that occur in hospitals; the 2004 report examined the incidence of serious safety issues in other settings as well, including ambulatory care facilities and nursing homes. It points out that earlier research on patient safety focused on errors of commission, such as prescribing a medication that has a potentially fatal interaction with another medication the patient is taking. The authors argue that errors of omission are equally important. An example of omission is failing to prescribe a medication from which the patient would likely have benefited (IOM, Committee on Data Standards for Patient Safety, 2004).

A significant contributing factor to the unacceptably high rate of medical errors reported in these two reports and many others is poor information management practices. Studies have shown that illegible prescriptions, unconfirmed verbal orders, unanswered telephone calls, and lost medical records can all place patients at risk.

Since the time the first IOM report was published, major purchasers of health care have taken a stand on improving the quality of care delivered in health care organizations across the nation. The Leapfrog Group, mentioned in Chapter One, has developed a list of criteria by which health care organizations may be judged in the future. One of the Leapfrog Group's many recommendations to improve patient safety is the widespread adoption of computerized provider order entry (CPOE) systems among health care organizations. CPOE systems will be discussed more fully in the next chapter, but in the context of today's health care information systems, they are a significant tool for decreasing errors made in the ordering and administration of medications and diagnostic and therapeutic tests.

Besides the need to address patient safety concerns and decrease medical errors, health care organizations face spiraling health care costs (including costs for prescription drugs), disparities of care, the need for better homeland security measures, nursing shortages, and increased regulation, including the need to comply with the HIPAA regulations. Many health care executives have come to realize that their organizations cannot survive and thrive without the effective use of information technology. Yet most of these executives find that their current health care information systems are grossly inadequate in improving quality, keeping patients safe, and decreasing costs. They often describe their organization's information systems as "fragmented" and "not able to communicate with each other." Many systems are redundant, resulting in "islands" of data that are

not well integrated across organizations, let alone within the individual organization. Clearly, there is an immediate need for uniform standards that will enable current systems and legacy systems to communicate with each other.

Despite the challenges of effectively implementing comprehensive health care information systems, and in particular clinical information systems, technologies are emerging that have the potential to ease some of the barriers and implementation issues of previous decades. The Internet continues to expand, as does the opportunity to bring systems together. *Wireless technology* is becoming more widely available and increasingly secure and promises the portability many providers demand. Several studies have shown that a growing number of physicians are using handheld computers, often referred to as *personal digital assistants* (PDAs), for a variety of purposes such as ready access to scheduling and calendar functions, drug information programs, and medical references (Figure 4.2). *Voice recognition*, although still not perfect, has come a

FIGURE 4.2. PHYSICIAN USING A PDA.



long way in the past few decades and has the potential to revolutionize the way providers enter data and interact with health care information systems. *Bar coding* has already been shown to be highly effective in identifying patients and in making sure that the right patient gets the right medication at the right time in the right dose. (These and other technologies will be discussed more fully in Chapter Eight.)

Why Health Care Lags Behind in Its Use of IT

One might wonder why, with all the advances in information technology, the health care sector has been slow to adopt health care information systems, particularly clinical information systems. Other industries have automated their business processes and have used information technology for years. The reasons for the slow adoption rate are varied and may not be readily apparent. First, health care information is complex, unlike simple bank transactions, for example, and it can be difficult to structure. Health care information may include text, images, pictures, and other graphics. There is no simple standard operating procedure the provider can turn to for diagnosing, treating, and managing an individual patient's care. Although there are standards of care and practice guidelines, the individual provider still plays a pivotal role in conducting the physical examination, assessment, and history of the patient. The provider relies on prior knowledge and experience and may order a battery of tests and consult with colleagues before arriving at a diagnosis or an individualized treatment plan. Second, health information is, by its very nature, *highly* sensitive and personal. What could be more sensitive than a patient's personal health habits, family history, mental health, and sexual orientation? Yet such information may be relevant to the accurate diagnosis and treatment of the patient. Every patient must feel comfortable sharing such sensitive information with health care providers and confident that the information will be kept confidential and secure. Until HIPAA, there were no federal laws that protected the confidentiality of all patient health information and the state laws varied considerably. The terminologies used to describe health information are also complex and are not used consistently among clinicians. Finally, the U.S. health care system is not a single system of care but rather a conglomeration of systems, including organizations in both the public and private sectors. Even within an individual health care organization there may be a number of fragmented systems and processes for managing information.

Another major challenge facing health care is the integration of heterogeneous systems. Some connectivity problems stem from the fact that when microcomputers became available and affordable in the last half of the 1980s, many health care organizations acquired department clinical systems with little regard for how they fit together in the larger context of the organization or enterprise. There was little emphasis

initially on enterprise-wide systems or on answering such questions as, Will the departmental systems communicate with each other? With the patient registration system? With the patient accounting system? To what degree will these systems support the strategic goals of the organization? As health care organizations merged or were purchased from larger organizations, the problems with integrating systems multiplied.

Integration issues may be less of an issue when a health care organization acquires an enterprise-wide system from a single vendor or when the organization itself is a self-contained system. For example, Hospital Corporation of America (HCA), a for-profit health care system comprising hundreds of hospitals throughout the nation, has adopted an enterprise-wide system from a single vendor that is used across all HCA facilities. However, rarely does a single vendor offer all the applications and functionality needed by a health care organization.

Summary

Health care information system is a broad term that includes both administrative and clinical information systems. An information system is an arrangement of information (data), processes, people, and information technology that interact to collect, process, store, and provide as output the information needed to support the health care organization. Administrative information systems contain primarily administrative or financial data and are used to support the management functions and general operations of the health care organization. Clinical information systems contain clinical, or health-related, information and are typically used by clinicians in diagnosing, treating, and managing the patient's care.

This chapter provided an overview of the history and evolution of health care information systems, including administrative and clinical applications, since the early 1960s. The information was presented in the context of the major events or issues that were pertinent to health care, changes in reimbursement practices, advances in information technology, and the federal government's growing interest in IT.

Although it is still too early to tell what the twenty-first century holds for health care information systems, if the past is any indication health care executives should keep abreast of major health issues and concerns, proposed changes to reimbursement practices, federal IT initiatives, and advances in information technology. The challenge health care organizations face is to overcome the barriers to the widespread adoption of information technology. To that end the following chapter describes a variety of clinical information systems, the major barriers to their widespread use, and the strategies health care organizations have employed to overcome these barriers.

Chapter Four: Learning Activities

1. Visit at least two *different* types of health care organizations, and compare and contrast the history and evolution of the information systems used within these respective organizations. What administrative information systems does each organization use? What clinical information systems? What factors led to the adoption or implementation of these systems? What role, if any, does the health care executive have in decisions about today's information systems (for example, the planning, selection, implementation, or evaluation of these systems)? Has this role changed over time? Explain.
2. Explore the history and evolution of at least *one* of the following information technologies. Create a timeline that includes its date of inception, major milestones, and use in and outside of health care.
 - a. Bar coding
 - b. Voice recognition
 - c. Wireless networks
 - d. Wireless devices (such as PDAs)
 - e. Digital imaging
 - f. Artificial intelligence
 - g. The Internet
 - h. Electronic mail (e-mail)
3. Choose a major federal policy initiative or piece of legislation that affects health care IT and describe the impact that it has had or will likely have in the future.
4. If the United States went to a single-payer model for health care, how would that affect providers' spending on health care IT? If the United States went to a payment mechanism in which reimbursement was based on the quality of care, how would that affect providers' spending on health care IT?
5. Examine the deployment of health care IT in the United Kingdom, Canada, or a European Union country. Why has health care IT evolved there in a way that is different from its evolution in the United States?



CHAPTER FIVE

CURRENT AND EMERGING USE OF CLINICAL INFORMATION SYSTEMS

What will it take to give U.S. health care organizations and providers access to comprehensive clinical information systems that are well integrated with administrative applications—not just in large academic medical centers but also in small community physician practices, nursing homes, and rural health clinics? Many health care organizations have already invested considerably in implementing administrative information systems and a handful of clinical applications. They are now wrestling with how to successfully expand their clinical information system capabilities in an effort to improve patient safety, increase quality, and decrease costs. Examples of clinical information system expansion include everything from computerized provider order entry (CPOE) systems to medication administration systems to fully electronic medical record (EMR) systems.

To appreciate the broad spectrum of clinical information system capabilities, this chapter begins by providing the reader with a conceptual framework for understanding the major components and functions of an electronic medical record system. We view the EMR as the *hub* of the organization's clinical information and as a tool in improving patient care quality and containing health care costs. Our discussion centers on the value of EMR systems to the patient, the provider, the health care organization, and the health care community at large. Other major types of health care information systems are also discussed, including two applications used to manage the patient care process within the health care organization (computerized provider order entry and medication administration) and applications used to deliver patient care services and to interact with patients at a distance (telemedicine and telehealth).

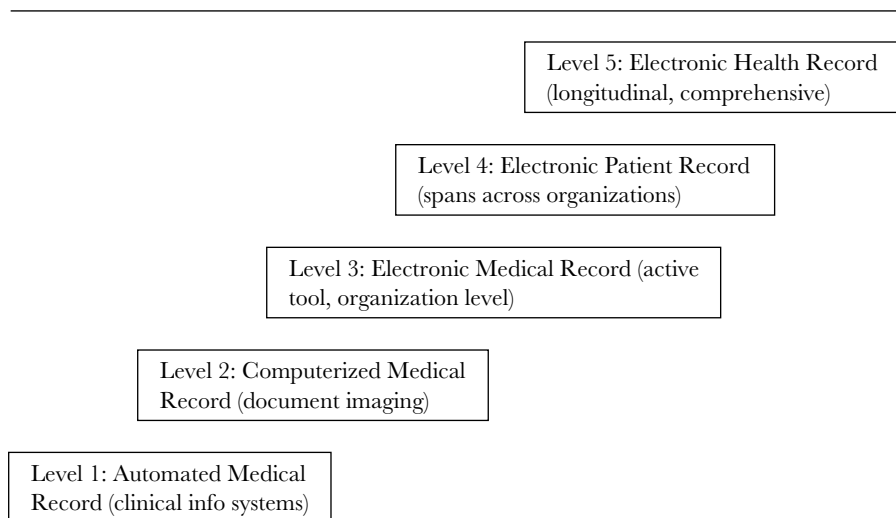
Implementing an EMR or any other health care information system in an organization does not happen overnight. It is a process that occurs over a number of years. Health care organizations today are at many different stages of IS adoption or implementation. We conclude this chapter by discussing barriers to adoption of health care information systems (financial, cultural, and technical), along with strategies that are being employed to overcome them.

The Electronic Medical Record

As we have discussed, patient medical records are used by health care organizations for documenting patient care, as a communication tool for those involved in the patient's care, and to support reimbursement and research. Most patient records have been kept, and are still kept, in paper form. Numerous studies have revealed the problems with paper-based medical records (Burnum, 1989; Hershey, McAloon, & Bertram, 1989; Institute of Medicine, 1991). These records are often illegible, incomplete, or unavailable when and where they are needed. They lack any type of active decision-support capability and make data collection and analysis very cumbersome. This *passive* role for the medical record is no longer sufficient in today's health care environment. Health care providers need access to *active* tools that afford them clinical decision-support capabilities and access to the latest relevant research findings, reminders, alerts, and other knowledge aids. The medical record of the future will likely become as critical to the accurate diagnosis and treatment of patients as the physician's stethoscope has been to detecting heart murmurs and respiratory problems.

Definition and Functions of EMR Systems

What are electronic medical records and how do they differ from merely automating the paper record? There are nearly as many different terms to describe electronic medical records as there are EMR-type systems available on the market today. In Chapter Four we introduced the concept of the EMR when we described the Institute of Medicine's definition of the CPR in its 1991 report titled *Computer-Based Patient Records: An Essential Technology for Health Care*. Since this IOM report was first published, a variety of terms have been used in the literature to describe systems of the EMR or CPR type. Given that there is no single universally used term or definition, we have chosen to use the definitions of the Medical Records Institute (MRI) when discussing the EMR and EMR-related systems (Waegemann, 1995, 1996). We selected this taxonomy because it defines the various levels, or stages, of computerizing health information and reflects the notion that EMR systems are acquired or developed over time (see Figure 5.1).

FIGURE 5.1. FIVE LEVELS OF COMPUTERIZATION.

Source: Waagemann, 1996.

Five Levels of Computerization. Following are descriptions of the Medical Records Institute's five levels of computerization.

Level 1: Automated Medical Record. At the first level, the *automated medical record*, the health care organization still depends on paper-based medical record systems, although nearly half of the patient information may be computer generated and stored as computer printouts within the medical record. The health care organization may automate certain functions such as patient registration, scheduling, results (radiology and laboratory) reporting, and dictation. However, at this level the paper-based medical record system remains the primary source for entering and retrieving the patient's clinical information, and the problems inherent in using paper records (availability, legibility, completeness) still exist. Automated medical records are managed by organizations.

Level 2: Computerized Medical Record. The next level, Level 2, involves digitizing the patient's medical record through the use of a document imaging system. Much of the patient's clinical information is scanned into the medical record and stored electronically as optical images. Document imaging systems may be used by organizations to address accessibility and retrieval concerns and space and storage issues associated with paper medical records. However, a document imaging system typically does not allow the user to analyze or aggregate data for decision-making purposes. It is merely a digitized

version of the paper medical record with some indexing and search capabilities. In other words, the *computerized medical record* has essentially the same structure as the paper-based medical record. Like the automated medical record, the computerized medical record is maintained by the organization. Many health care organizations opt not to use document imaging systems. They see them as a costly storage medium and as an unnecessary step in getting to the next level, the electronic medical record.

Level 3: Electronic Medical Record. Up until this point the medical record has served as a passive storage device. It is at Level 3, the *electronic medical record* (EMR), where we begin to see the patient record as an *active* tool that can provide the clinician with decision-support capabilities and access to knowledge resources, reminders, and alerts. Although still used and maintained at the organizational level, the EMR provides the clinician with access to decision-support capabilities and other aids. For example, the EMR may alert the clinician to the fact that the patient is allergic to certain medications or that two medications should not be taken in combination with each other (Figure 5.2). It may trigger a reminder that the patient is due for a health maintenance test such as a mammography or cholesterol test (Figure 5.3).

A recent letter report by the Institute of Medicine (IOM, Committee on Data Standards for Patient Safety, 2003a) expands on the MRI's definition of the EMR and identifies the following core components:

FIGURE 5.2. SAMPLE DRUG ALERT SCREEN.

Test, Jill		CLB3	
(10433415 CRM)		PHS INFO SYSTEMS	
Select	Desktop	Pt Chart: Medications	Oncology Custom Reports Admin Sign Results Resource Popup

Warning

You are ordering: AMOXICILLIN

Drug - Allergy Intervention

Alert Message The patient has a documented allergy: Penicillins. Reaction: Unknown.	Keep New Order - select reason(s) ☐ Patient does not have this allergy, will D/C pre-existing allergy Reasons for override: ☐ Patient has taken previously without allergic reaction ☐ Low risk cross sensitivity, will monitor ☐ No reasonable alternatives ☐ Other

Local intranet

Source: Partners HealthCare System, Inc.

- *Health information and data*: includes defined data sets such as medical and nursing diagnoses, a medication list, allergies, demographics, clinical narratives, and laboratory test results
- *Results management*: manages all types of results (for example, laboratory test results, radiology procedure results) electronically
- *Order entry or management*: incorporates use of computerized provider order entry, particularly in ordering medications
- *Decision support*: employs computerized clinical decision-support capabilities such as reminders, alerts, and computer-assisted diagnosing
- *Electronic communication and connectivity*: enables those involved in patient care to communicate effectively with each other and with the patient; technologies to facilitate communication and connectivity may include e-mail, Web messaging, and telemedicine
- *Patient support*: includes everything from patient education materials to home monitoring to telehealth
- *Administrative processes*: facilitates and simplifies such processes as scheduling, prior authorizations, insurance verification; may also employ decision-support tools to identify eligible patients for clinical trials or chronic disease management programs
- *Reporting and population health management*: establishes standardized terminology and data formats for public and private sector reporting requirements

FIGURE 5.3. SAMPLE EMR SCREEN.

Claus, Santa

4047482 (MGH) 01/01/1901 (103 yrs.) M

JPG0 PHS INFO SYSTEMS

Select Desktop Pt Chart: Summary Oncology Custom Reports Admin Sign Results Resource Popul

Reminders

- Patient is 50 years old or older, recommend Influenza vaccination

Problems Add New

Hypertension [N]
Diabetes mellitus [N]
F/h obesity - Major
Gout [N]
Back pain

Medications Add New

Amoxicillin 250MG 1 TID
Ativan 1MG 1 Q4H [N]
Bacrim ds 1 BID [N]
Compazine 10MG 1 Q6H [N]
Decadron 4MG 5 6 and 12 hours before chemo [N]

Allergies Add New

Nkda [N]

Procedures Add New

Deviated nasal septum

Vital Signs

09/14/2003 BP 120/90 P N/A
RR N/A Temp N/A
HT N/A WT N/A

Health Maintenance

Notes

Fam/Soc History

Visits

Done Local intranet

Source: Partners HealthCare System, Inc.

To support these components, the health care organization should have in place (1) an organization-wide system for identifying patients; (2) a mechanism for providing all clinicians involved in the patient's care with access to relevant clinical information; (3) a common workstation, including common medical record software, structures, and interfaces; and (4) a security system that monitors who has access to patient information and electronic signatures and that has the ability to ensure data quality or integrity (for example, it has auditing capabilities that ensure no loss or alteration of information after editing).

How clinicians interact with or use the EMR may be quite different from how they used paper-based medical records. For example, providers may use the EMR for generating prescriptions, referencing drug alerts, and sending patient reminder notes. To enable these functions, the health care organization must have an appropriate infrastructure to capture, process, and store the information. Later in the chapter we will discuss the use of EMR systems in health care organizations. At this point, it is important to understand how an EMR fundamentally differs from an automated medical record and a computerized medical record system—it is an *active* tool for managing patient care.

Level 4: Electronic Patient Record. Whereas the electronic medical record contains only the patient information that is maintained by a single organization, the *electronic patient record* (Level 4) includes all health care–related information concerning the patient—gathered across two or more organizations. An electronic patient record brings together in a central database all clinical information available on a patient. For example, if a primary care physician saw a patient in the physician's office, admitted the patient to a hospital, and then discharged the patient to a rehabilitation facility, all relevant information concerning the patient would be available to clinicians involved in the patient's care across these three settings. This level of computerization requires (1) a system of identifying all patient information available, (2) a way to combine information from multiple facilities, (3) a common terminology and structure, and (4) a consensus on security. The electronic patient record system is comparable in its scope and functions to the CPR (discussed earlier) as defined by the IOM in 1991.

Level 5: Electronic Health Record. The *electronic health record* (EHR) (Level 5) is broader in scope than the electronic patient record and includes wellness information and other information not routinely maintained by health care organizations. Wellness information might include data on the individual's smoking habits, nutrition, level of exercise, dental health, and alcohol use. The patient is at the center and all information related to the individual's health and wellness is brought together as needed in managing the patient's care and treatment more effectively. The EHR is a longitudinal record and ultimately would encompass a person's relevant health information from before birth to death.

Key Points—MRI's Five Levels of Computerization. There are several key points to keep in mind in reviewing the MRI's five levels of computerization. First, the levels are not intended to be necessarily linear nor sequential. For example, a health care organization does not have to employ a document imaging system (Level 2) to implement an EMR system (Level 3). The levels do, however, illustrate the fact that adoption of EMR-type systems is evolutionary and occurs over time. The ultimate goal may be to develop and implement information systems that provide clinicians with a comprehensive view of the patient's health and well-being. Health care organizations do not move from entirely manual paper-based systems to the EHR overnight. Most organizations currently employ some level of computerization of clinical information. For instance, they may capture patient registration information or results from laboratory tests and radiology exams electronically. They may wish to expand their use of information technology and automate the ordering process or institute a bar-coding system for identifying patients and medications. These five levels are simply one method for describing the degree of computerization used in managing health information.

Second, the first three levels all pertain to the computerization of patient information at the *organizational* level. It is not until Level 4 that we see the sharing of information across organizations. For simplicity, we use the term *EMR* to refer to organizational systems and *EHR* to refer to systems that share information across organizations. There are a host of challenges associated with getting different clinical applications to interoperate or share information with each other. This task can be even more daunting when one attempts to share information across organizational settings. Technical standards are needed as well as uniform definitions of data. The need for standards and some of the initiatives that are currently under way to develop standards are discussed briefly at the end of this chapter and further in Chapter Nine.

Finally, the EMR (and the EHR) is quite different from merely automating the paper medical record. The EMR is an *active* tool that is used by the clinician to manage the patient's care. It provides decision-support capabilities, access to reminders and alerts and other knowledge aids—all functions that are not possible with paper-based systems. Because there is no universal definition of the EMR, some health information system vendors or providers will refer to document imaging systems (Level 2) as electronic medical record systems (Level 3). It is important to point out that document imaging systems are not the same as the EMR as defined here. Document imaging systems are an electronic storage means for organizing and maintaining medical records. EMR systems have far more capability for searching records than document imaging systems do, enable aggregate data to be generated, and serve as an active decision-making tool to the provider in managing patient care. This is an important distinction that should be considered when exploring the adoption of EMR-type systems in a health care organization.

Current Use of EMR Systems

How widely are EMR systems used in hospitals, physician practices, and other health care organizations? A recent report by Brailer and Terasawa (2003) suggests that EMR adoption and use rates are difficult to assess. Part of the difficulty stems from the fact that many of the relevant studies have employed retrospective, nonrandom, subjective recall surveys. The lack of a universally used definition for the EMR (or CPR or EHR) and lack of agreement on what functions or features are part of an EMR add to the difficulty of drawing conclusions from the studies that have been done. Estimates on EMR adoption in hospitals range from 5 to 13 percent, with another 25 percent of respondents reporting that their hospitals plan to use EMR in the near future. This compares with EMR usage estimates ranging from 14 to 39 percent for physician office settings (Brailer & Terasawa, 2003). EMR usage rates in other settings are not widely known.

Although there are problems inherent in the methods used to determine adoption rates, it is probably safe to say that between 5 to 10 percent of hospitals and 15 to 20 percent of physician practices currently use EMR systems. These percentages are low compared to EMR usage in other countries. More than half of all primary care physicians are estimated to use EMR systems in countries such as Austria, Finland, Denmark, the Netherlands, and Sweden (Brailer & Terasawa, 2003). It is worth noting that these countries all have either a single-payer system or a government that mandates EMR use.

Factors Influencing EMR Adoption

Despite the low rates of EMR use in the United States, a number of factors are driving an increased interest in adopting such systems. A recent study by the Medical Records Institute (2004c) ranked these factors by perceived likely relevance, with the highest-ranked factor listed first. Felt to be significant in influencing health care organizations and providers to adopt EMR systems now or in the near future is the desire to

- Improve clinical processes or workflow efficiency
- Improve quality of care
- Share patient record information among health care practitioners and professionals
- Reduce medical errors (improve patient safety)
- Improve clinical data capture
- Improve clinical documentation to support appropriate billing service levels
- Provide access to patient records at remote locations
- Facilitate clinical decision support
- Meet the requirements of legal, regulatory, or accreditation standards
- Contain or reduce health care delivery costs
- Establish a more efficient and effective information infrastructure as a competitive advantage

Health care organizations and providers are discovering that EMR systems are needed if they are to more efficiently and effectively deliver health care services. They are also becoming increasingly aware of the value of EMR systems to the patient, the provider, the organization, and the health care community at large in improving quality, addressing patient safety concerns, and decreasing administrative costs.

Value of EMR Systems

Numerous studies over the past twenty years have demonstrated the value of using EMR systems and other types of clinical information systems. In a report prepared for the Kaiser Permanente Institute for Health Policy, the authors found that the benefits could be categorized into three major classes: (1) improved quality, outcomes, and safety; (2) improved efficiency, productivity, and cost reduction; and (3) improved service and satisfaction (Raymond & Dold, 2002). Following is a discussion of each of these major categories of benefits, along with several examples illustrating the value of EMR systems to the health care process.

Improved Quality, Outcomes, and Safety. Clinical information systems can have a profound impact on patient quality, outcomes, and safety. Several studies have shown that physicians who had access to clinical practice guidelines and features such as computerized reminders and alerts were far more likely to provide preventive care than were physicians who did not (Balas, Weingarten, Garb, Blumenthal, Boren, & Brown, 2000; Bates, Kuperman, et al., 1999; Kuperman, Teich, Gandhi, & Bates, 2001; Teich, Merchia, Schmiz, Kuperman, Spurr, & Bates, 2000; Ornstein, Garr, Jenkins, Rust, & Arnon, 1991). Other studies have found that computerized reminders used in an outpatient setting can have a significant effect on cancer prevention activities such as the performance of stool occult-blood tests, rectal examinations, breast examinations, smoking cessation counseling, and dietary counseling (Landis, Hulkower, & Pierson, 1992; McPhee, Bird, Jenkins, & Fordham, 1989; McPhee, Bird, Fordham, Rodnick, & Osborn, 1991; Yarnall et al., 1998). EMR-related systems have also been shown to improve drug prescribing and administration by providing clinicians with information regarding the appropriate use of antibiotics at the point of care (Berman, Zaran, & Rybak, 1992), reducing adverse drug reactions (Bates & Gawande, 2003; Evans, Pestotnik, Classen, & Burke, 1993; Burke & Pestotnik, 1999), improving the accuracy of drug dosing (Duxbury, 1982), and reducing errors of omission such as failing to act on results or to carry out indicated tests (Bates & Gawande, 2003; Litzelman, Dittus, Miller, & Tierney, 1993; McDonald et al., 1984; Overhage, Tierney, Zhou, & McDonald, 1997). A recent report by Bates and Gawande (2003) states that information technology can reduce the rate of medical errors by (1) preventing errors and adverse effects, (2) facilitating a more rapid response after an adverse event has

occurred, and (3) tracking and providing feedback about adverse effects. Likewise, EMR-type systems can improve communication, make knowledge more readily available, require key pieces of information (such as the dose of the drug), assist with calculations, perform checks in real time, assist with monitoring, and provide decision support. If effectively incorporated into the care process, all of these features have the potential to improve quality, outcomes, and patient safety.

Improved Efficiency, Productivity, and Cost Reduction. In addition to improving the quality of care the patient receives, studies have shown that the EMR can improve efficiency, increase productivity, and lead to cost reductions (Barlow, Johnson, & Steck, 2004; May, 2002; Overhage et al., 2002; Tate, Gardner, & Weaver, 1990; Tierney, Miller, Overhage, & McDonald, 1993). It is not uncommon for clinicians who do not have EMR access to order a second set of tests because the results from the first set are unavailable, so one way EMR systems improve efficiency is by making test results readily available to clinicians (Bates, Kuperman, et al., 1999; Tierney, McDonald, Hui, & Martin, 1988; Tierney, Miller, & McDonald, 1990). In addition, EMR features such as computerized reminders and alerts can reduce pharmaceutical costs by prompting physicians to use generic and formulary drugs (Bates & Gawande, 2003; Donald, 1989; Garrett, Hammond, Stead, 1986; Levit et al., 2000; Karson, Kuperman, Horsky, Fairchild, Fiskio, & Bates, 1999).

Several studies have shown that the use of EMR systems can save physicians time in the long run and can reduce costs related to the retrieval and storage of medical records. For instance, the Memorial Sloan-Kettering Cancer Center estimated that it realized space savings of 2,000 square feet after implementing an EMR, equating to a savings of approximately \$100,000 a year (Evans & Hayashi, 1994). Savings have also been realized through the decreased use or elimination of transcription services (Renner, 1996). Others have reported that an EMR has led to higher-quality documentation, resulting in improved coding practices and subsequently higher reimbursement (Barlow, Johnson, & Steck, 2004; Bleich, Safran, & Slack, 1989; Wager, Lee, White, Ward, & Ornstein, 2000) and also in savings from lower drug expenditures, improved utilization of radiology tests, and decreased billing errors (Wang et al., 2003). In fact, one multispecialty, fifty-nine-physician group practice estimates that it will save a total of \$8.2 million over the next five years as a result of its EMR system (Barlow et al., 2004).

Improved Service and Satisfaction. The third category of benefits to be realized as a result of using EMR systems includes improved service and satisfaction, from both the patient's and the user's perspective. Patients whose physicians use EMR systems like the fact that their health information (health history, allergies, medications, and test results) is readily available when and where it is needed. Several qualitative studies have

shown that patients' response to physicians' using an EMR in the examination room have been quite positive (Ornstein & Bearden, 1994; Ridsdale & Hudd, 1994). Patients in practices that use an EMR system view their physicians as being innovative and progressive. And even though some physicians initially expressed concern that using the EMR in the examination room might distance them from patients or impede the physician-patient relationship, the majority by far of the studies in this area have shown that the EMR has had no negative impact on the physician-patient relationship (Gadd & Penrod, 2000; Haddad, Potvin, Roberge, Pineault, & Remondin, 2000; Legler & Oates, 1993; Solomon & Dechter, 1995) and can in fact enhance it by involving patients more fully in their own care (Marshall & Chin, 1998).

EMR-type systems can also positively affect provider and support staff satisfaction. Physicians who have successfully implemented an EMR system in their practice have reported that it has improved the quality of documentation, improved efficiency, and had a positive impact on their job satisfaction and stress levels (Wager et al., 2000). They are proud of the quality of their records and believe that their documentation is now more complete, accurate, and available and more useful in substantiating the diagnostic and procedural codes assigned for billing purposes. EMR users such as nurses and support staff have reported that the EMR has enhanced their ability to respond to patient questions promptly. Support staff who have historically been responsible for filing paper reports, pulling paper records, and processing bills, tout the many benefits of having easy access to patient information through the use of an EMR system (Wager et al., 2000).

There are many examples of health care organizations that have successfully implemented EMR systems and have realized the value that comes from using them. Figure 5.4 profiles the 2003 Nicholas E. Davies Award recipient in the primary care practice category; Figure 5.5 profiles the 2003 recipient in the organizational category. The Nicholas E. Davies Award was established in 1994 by the Computer-Based Patient Record Institute (CPRI) to recognize organizations that have carried out exemplary implementations of EMR systems. (The Healthcare Information and Management Systems Society [HIMSS] has administered the Davies award since 2002, the year that CPRI merged with HIMSS.)

Other Major Types of Health Care Information Systems

In addition to EMR systems, several other clinical information systems or applications warrant further discussion. The four we have selected to discuss are computerized provider order entry (CPOE), medication administration, telemedicine, and telehealth. We selected these systems because (1) they have an enormous potential to improve quality, decrease costs, and improve patient safety or (2) they are being widely debated and are likely to be hot topics for the next few years—or they possess both these qualities.

FIGURE 5.4. PROFILE OF THE 2003 NICHOLAS E. DAVIES AWARD RECIPIENT: PRIMARY CARE PRACTICE CATEGORY.

Recognized as the winner of the 2003 Davies Award for Primary Care Practice by the Healthcare Information and Management Systems Society (HIMSS), Roswell Pediatric Center, with three offices around Atlanta, Georgia, successfully implemented an electronic health record (EHR) into the routine care and operation of its practice, which resulted in substantial improvements in efficiency, its quality, and in staff and patient satisfaction.

In 2001, Roswell began looking for an EHR that would easily interface with its existing practice management and billing systems. After a well-planned and -executed search process, Roswell decided on a system designed and implemented by Noteworthy Medical Systems that met its interfacing needs and would automate several routine processes. Because the implementation was met with staff acceptance and the system was inherently easy to use, Roswell was able to smoothly transition its paper-based practice to an EHR.

The EHR is a complete point-of-care documentation, charge capture, and decision-support system which has completely redesigned the workflow and processes of the practice, which resulted in improved workflow, communication, and patient care. Roswell estimates that this system has allowed the practice to cut six hours of staff time that was dedicated to manual data entry as well as decrease the 440,000 charts pulled annually to nearly zero. Financially, Roswell has been able to capture the 18 percent of charges for services that were lost before the implementation of the EHR. These benefits, in addition to the primary goals of improving workflow, communication, and patient care, have allowed Roswell to realize significant economic gains.

With its new EHR in place and operating smoothly as part of Roswell's daily operations, the practice is well positioned for future growth, increased quality of patient care, and continued financial and economic gain.

Source: Adapted from HIMSS, 2004.

The first two, computerized provider order entry and medication administration systems, are applications used primarily in health care settings where tests and medications are ordered, performed, or administered. The last two, telemedicine and telehealth, are means of delivering services or communicating with patients at a distance. Each of these information systems is described in the sections that follow, along with their current use and value to the patient care delivery process.

Computerized Provider Order Entry

One of the biggest concerns facing health care organizations today is how to keep patients safe. Several Institute of Medicine studies have brought to the forefront of people's attention the fact that an estimated 98,000 patients die each year in U.S.

**FIGURE 5.5. PROFILE OF THE 2003 NICHOLAS E. DAVIES AWARD
RECIPIENT: ORGANIZATIONAL CATEGORY.**

Cincinnati Children's Hospital Medical Center (CCHMC), a 373-bed not-for-profit pediatric specialty hospital, has taken the use of its EMR system to new levels of influence, usage, and effectiveness. CCHMC has implemented Integrating Clinical Information Systems (ICIS) which comprises several integrated systems including: Picture Archiving and Communication System (PACS); a clinical discharge summary system, which allowed physicians for the first time to enter important information directly into an information system; a Web-based patient results system, which provides secure access to patient test results from anywhere in the system; computerized provider order entry (CPOE) with built-in safety checks to minimize dosage errors due to improper weight entries, medication under- or overdosing, medication allergies or interactions, and duplicate orders; and a clinical documentation system.

CCHMC's ongoing commitment to the development and implementation of its EMR has had a positive impact on patient care, patient safety, efficiency, the cost of health care, regulatory compliance, and patient satisfaction. The implementation has resulted in a 35 percent reduction in medication errors and a 52 percent improvement between the time medicines are ordered and the time they are ready to be given to patients. X-ray images are delivered electronically, eliminating the need for films, and urgent X-rays arrive much quicker than before. Doctors and nurses have information available at their fingertips, allowing them to make quicker and more accurate clinical decisions. Patients with chronic illnesses can access their health records over a secure Internet connection from anywhere in the world.

ICIS is now expanding to include chronic care portals—web-based applications to help families whose children have chronic diseases manage their own care—often from distances far from Cincinnati. The portals graphically depict test results, trends, and other medical information, and provide secure communication between patients and clinicians. Patients and their families can access the on-line, browser-based system from anywhere in the world. In addition, Cincinnati Children's is implementing a new perioperative, anesthesia, and intensive care electronic information system. This system will serve as “mission control” for these critical patient care areas—tracking a child's progress at every step of the way—from surgery registration to recovery to critical care. Doctors and nurses will be able to view a child's status at any given moment, see exactly what happened at previous steps, and gain access to the patient's complete medical history .

Source: Adapted from HIMSS, 2004.

hospitals due to medical errors (IOM, 2000, 2001). Medication errors and adverse drug events (ADEs) top the list and are common, costly, and clinically important issues to address. A *medication error* is an error in the process of ordering, dispensing, or administering a medication, whether or not an injury occurs and whether or not the potential for injury is present. An *adverse drug event* is an injury resulting from the use of a drug, a use that may or may not have involved a medication error. Thus a medication error may lead to an adverse drug event, but does not necessarily do so (Bates, Teich, et al., 1999). Studies have shown that computerized provider order entry (CPOE) has the potential to reduce medication errors and adverse drug events (Bates et al., 1998; Evans et al., 1998; Bates & Gawande, 2003). In fact the Leapfrog Group (2004a) has identified CPOE as one of three changes that it believes would most improve patient safety.

Many health care executives have taken steps to implement CPOE or are planning to do so in the near future. What is CPOE? How might it improve patient safety? How widely used are CPOE systems? We begin by defining CPOE and its major functions, then move on to discuss its current use and its potential value in improving patient safety and preventing medical errors.

Definition and Primary Functions of CPOE Systems. During a patient encounter, the physician generally orders a number of diagnostic tests and therapeutic plans for the patient. In fact, virtually every intervention in patient care—performing diagnostic tests, administering medications, drawing blood—is initiated by a physician's order. Historically, physicians have handwritten these orders or called them in as verbal orders for a nurse or other health care professional to document. The ordering process itself is a critical step in the patient care process and represents a point where intervention can often prevent medication errors and improve adherence to clinical practice guidelines (First Consulting Group, 2003).

CPOE, at its most basic level, is a computer application that accepts physician orders electronically, replacing handwritten or verbal orders and prescriptions. Most CPOE systems provide physicians with decision-support capabilities at the point of ordering. For example, an order for a laboratory test might trigger an alert to the physician that the test has already been ordered and the results are pending. An order for a drug to which the patient is allergic might trigger an alert, warning the physician of the patient's allergy and possibly recommending an alternative drug. If a physician orders an expensive test or medication, the CPOE might show the cost and offer alternative tests or drugs. CPOE systems can also provide other types of clinical decision support to the physician. For instance, if the physician is ordering a series of tests and medications for a common diagnosis, the computer can offer the use of a preprogrammed, institutionally approved set of orders to facilitate the process and can recommend drug therapy to aid the physician in following accepted protocols for that

diagnosis (Metzger & Turisco, 2001) (Figure 5.6). The scope of CPOE functions and capabilities can vary considerably. The most advanced systems have sophisticated decision-support capabilities and can aid the provider in diagnosing and treating the patient by supplying information derived from knowledge-based rules and the latest research.

Current Use of CPOE. Estimating the current use of CPOE systems is almost as difficult as assessing the use of EMR systems. A CPOE system is typically an integral part of a comprehensive clinical information system or EMR system and not a stand-alone application. Most of the recent estimates of CPOE use in hospitals put it at approximately 5 percent (Leapfrog Group, 2002; First Consulting Group, 2003). Many academic health care centers have adopted existing inpatient CPOE systems to the ambulatory care arena. A more recent report by Brailer and Terasawa (2003) suggests that the overall usage rates are likely close to 13 percent, comparable to the use of EMR systems.

FIGURE 5.6. SAMPLE CPOE SCREEN.

Source: Partners HealthCare System, Inc.

A recent HIMSS survey found a direct relationship between organization size and CPOE use. That is, larger organizations, those with annual budgets greater than \$500 million, were far more likely to be implementing CPOE systems than health care organizations with annual budgets of less than \$100 million. Smaller organizations reported that they had no current plans to implement CPOE systems (HIMSS, 2003a). Why the relatively low usage rate? Part of it may be due to the fact that historically, health care executives and vendors did not believe that physicians would be interested in computerized order entry, and consequently CPOE development lagged behind the development of other clinical information system components. Even among hospitals that have implemented a full or partial CPOE system, less than 14 percent require physicians to use the system (Ash, Gorman, Lavelle, Lyman, & Fournier, 2001).

Value of CPOE. Despite the relatively low usage rates, CPOE systems can provide patient care, financial, and organizational benefits. Clearly, one of the fundamental reasons that CPOE has received so much attention in recent years is its potential to improve patient safety and, more specifically, reduce medication errors. One controlled trial involving hospital inpatients reported a 55 percent reduction in serious medication administration errors following the introduction of a CPOE system (Bates et al., 1998). This particular CPOE system was developed in-house and improved communication, provided knowledge aids to physicians (including information on appropriate constraints on choices of medications, routes, frequencies, and doses), helped with calculations, performed real-time checks, and assisted in monitoring patients' conditions. A subsequent study of the same system found an 83 percent reduction in the overall rate of medication errors (Bates, Miller, et al., 1999).

The benefits of using CPOE systems are not unique to hospitals. Two recent reports (Johnston, Pan, Walker, Bates, & Middleton, 2003, 2004) brought national attention to the benefits to be gained from using CPOE systems in ambulatory care settings. The authors found that from a clinical perspective, CPOE produces better adherence to clinical protocols and improvements in the stages of clinical decision making (that is, initiation, diagnosing, monitoring and tracking, and acting). They also found that CPOE can lead to improved patient outcomes by reducing medical errors, decreasing morbidity and mortality, and expediting recovery times. A report from the Agency for Healthcare Research and Quality (2001) substantiates the notion that CPOE systems can significantly reduce medication errors and estimates that such systems may prevent 28 percent to 95 percent of adverse drug events.

Besides the clinical and patient care benefits, CPOE systems can also provide financial benefits to a health care organization. For example, organizations that use ambulatory CPOE systems may require fewer administrative clinical staff, improve

the accuracy and timeliness of billing, and increase transaction processing rates (Johnston et al., 2004). Other financial benefits include increased procedure volume and reductions in average length of stay.

Finally, a host of organizational benefits arise from using CPOE systems. Some health care organizations that use CPOE systems have found that their providers and patients are highly satisfied with their access to health care information, their wait times, and the quality of care delivered (Johnston et al., 2003) (Figure 5.7).

CPOE systems clearly have enormous potential for a positive impact on patient care and the delivery process. However, as with EMR systems, a host of challenges must be overcome if these systems are to be widely used in health care. Several prestigious organizations have had their share of CPOE challenges, despite their best efforts. For instance, in the late 1980s the University of Virginia experienced a great deal of resistance to its CPOE initiative. Leadership underestimated the impact of CPOE on clinical workflow as well as on physicians' and nurses' time and, in retrospect, did not invest sufficient resources in the effort. Many physicians, including residents, perceived the CPOE as an Information Systems Department initiative rather than as a clinician-led effort and felt it was forced upon them with little flexibility. Physicians complained administration was trying to "turn them into clerks and save money." Cumbersome interfaces and time-consuming ordering processes, along with the fact that the clinical care processes were never fully redesigned, contributed to the problems encountered (Massaro, 1993a, 1993b). In 2003, Cedars Sinai in Los Angeles experienced some of the same problems with its CPOE system implementation and ended up "pulling the plug" on the system, as the following case study describes.

FIGURE 5.7. PROJECTED BENEFITS OF IMPLEMENTING ADVANCED AMBULATORY CPOE SYSTEMS.

- **Improved Patient Outcomes**

Nationwide adoption of advanced ambulatory CPOE systems will eliminate more than 2 million adverse drug events and more than 190,000 hospitalizations per year.

- **Cost Savings**

Nationwide adoption of advanced ambulatory CPOE systems will save the U.S. health care system approximately \$44 billion per year in reduced medication, radiology, laboratory, and adverse drug event-related expenditures.

- **Provider Revenue Enhancement**

Using advanced ambulatory CPOE systems, providers can eliminate more than \$10 in rejected claims per outpatient visit.

Perspective: CPOE Implementation

Cedars-Sinai Medical Center developed and implemented a computer system known as Patient Care Expert (PCX) several years ago as part of a larger project to modernize the medical center's computing infrastructure. The PCX system included a CPOE component and used browser-based technology, making the system accessible through any browser-enabled computer anytime, anywhere. Other performance criteria specified that

- "The system needed to be highly flexible, allowing for rapid modifications of content and functionality."
- "The system needed to be fully integrated with all ancillary services, patient registration and patient accounting."
- "The system needed to be user-friendly for large groups of users with a diverse range of familiarity and experience with computers" (Langberg, 2004).

After conducting an extensive review of existing products and obtaining broad input from administration, clinicians, and information technology experts, the Cedars-Sinai board of directors decided the organization should develop an in-house product in collaboration with Perot Systems. In August 2002, after nearly three years of development and testing, Cedars-Sinai launched a pilot program of the PCX system. This pilot involved obstetrical patients over a two-week period, during which approximately 400 patients were entered into the system. As part of the pilot, more than 140 physicians and 200 department staff members used the system to care for all obstetrical patients. Clinical staff tested the system with more than 20,000 orders. By October, more than 2,000 physicians had been trained and certified to use PCX. The pilot was felt to have been very successful, and minor changes were made to the PCX before rolling it out to other areas of the medical center. By January 2003, 700,000 orders had been placed for more than 7,000 patients—more than 10,000 orders per day. The system was operational for more than two-thirds of the medical center's inpatients. However, in late January 2003, the system was suspended after hundreds of physicians complained that the system slowed down the ordering process and said they feared that orders were getting lost in the system. The medical center had worked with a forty-physician medical executive committee throughout the development and implementation process, and the administration believed that physicians were sufficiently involved throughout the project. However, rank-and-file physicians argued that the committee did not represent their views (Chin, 2003). One physician, for example, argued that the CPOE was very cumbersome and didn't follow physician workflow. This same physician complained that to order an antibiotic, doctors had to go through three or four different computer screens and wait six to eight seconds between screens (Chin, 2003). After receiving such complaints, the administration made the decision to take down the CPOE system. Those involved in

the implementation reported that they found themselves managing two complex processes:

1. *“Physician change management:* Four months into ‘go-live’ physicians remained deeply concerned about the added time they reported in entering orders and their negative perception of the system’s ease of use. Further, [it was] believed that too many physicians . . . did not have an optimal working knowledge of the system’s functionality.”
2. *“Workflow change management:* The procedures involved in hospital-based patient care are complex in any environment and need to be carefully and thoroughly understood in advance of automation. Additionally, CPOE will affect the workflow of all caregivers. [It was found that] far more operational workflow analysis and adjustment needed [to occur] after the ‘go-live,’ than was initially anticipated” (Langberg, 2004).

Besides managing these two processes, the management team has instituted a number of system enhancements and has aggregated input from all users to enhance PCX and improve the implementation and workflow procedures. By intensifying training and support resources, and accelerating the system response time, management expects to improve physicians’ experiences.

Adapted from Langberg, 2004

We will discuss a host of issues related to the implementation of CPOE and other health care information systems more fully in Chapter Seven. At this point, however, it is important to understand that CPOE systems can have a dramatic impact on physicians—how they spend their time, their work patterns, and the functions they perform. Most successful CPOE implementations have found that it takes physicians the same or more time to place orders with a CPOE system as it does to handwrite orders (Bates, Kuperman, & Teich, 1994). Additional time is often needed due to the decision-support features, which may require detailed information from the physician. CPOE is not simply a niche computer system to replace handwritten orders. Rather, it is a tool to aid the provider in order management. It can directly affect not only physician ordering but also physician decision making (through the decision-support features) and care planning, pharmacist decision making and workflow, nursing workflow and documentation, and communication with ancillary services (Sittig & Stead, 1994). Just as automating the paper medical record is not the same as implementing an EMR system, neither is automating the ordering process the same as implementing a CPOE system. Like an EMR system, a CPOE system provides decision support and can be a useful tool to the provider in managing the patient’s care more effectively, as the following example illustrates.

Perspective: CPOE and Decision Support

A study published by Teich et al. (2000) investigated the effects of computerized physician order entry (CPOE) on prescribing practices in a large urban academic medical center. Looking at several different earlier research studies, the investigators found substantial evidence that a CPOE system, which has the ability to make therapeutic recommendations at the exact time of order entry based on predetermined and accepted clinical guidelines, can increase the quality of care provided in a health care setting by reducing medication errors such as underprescribing, overprescribing, incorrect choice of drugs, and failure to recognize adverse effects of a particular drug therapy.

The researchers performed a time series analysis of orders entered through a computerized system that displayed drug use guidelines; offered complementary, substitute, or alternate therapies; and suggested appropriate prescribing practices at the time of entry. At the conclusion of the study and in one- and two-year follow-ups of the study, Teich et al. found that CPOE was a powerful and effective tool for improving prescribing practices of physicians at the study site. The change in prescribing practices resulted in both an improvement in care in the study institution as well as a reduction in costs.

The investigators point out an important fact regarding CPOE: the computerized system is only a tool and is not the decision maker or the final determinant of a course of treatment. It is the ultimate responsibility of the physician to make the final decisions for treatment plans and to use the computerized system only as a reference or guide. The study notes that physicians are willing to accept an alternate treatment or suggestion made by the system as long as the system does not automatically change the plan of treatment. The CPOE system must not make changes to orders without approval by the physician, thereby giving the physician the final decision in submitting an order.

According to the study, implementing a CPOE system requires major process change and can be difficult and expensive. Physicians are more willing to accept this change if and only if the system is well designed, adds value, and is properly managed during both preimplementation (training) and postimplementation (technical and functional support) stages. Moreover, the system must be viewed by physicians as a tool to improve care and not as a device by which their performance is monitored.

The investigators conclude decisively that CPOE, supplemented by clinical decision support, is a useful and powerful tool for improving physician prescribing. In order for CPOE to be effective in an institution, a partnership between the physician and the computer, coupled with high levels of human communication, must be formed. Once this occurs, CPOE will yield great results including the promotion of optimal care decisions, the prevention of adverse events, an increase in compliance with predetermined and accepted clinical guidelines, and a reduction in the cost of health care.

Medication Administration Systems

Another clinical application that is being widely discussed in terms of its potential to improve patient safety is medication administration that uses *barcode-enabled point of care* (BPOC). Like EMR and CPOE systems, medication administration systems with BPOC have the potential to address many patient safety issues, particularly those relating to correctly identifying patients and medications. Patient safety is such a complex issue that it is very unlikely that it can be fixed by a single solution. The HIMSS Bar Coding Task Force argues that “unprecedented cooperation through the medical supply chain, across software vendors and within provider organizations, is required” (HIMSS, 2003b, p. vii) for real change to occur.

Bar-coding technology is nothing new. It has infiltrated our lives, and we find it in grocery stores, hospitals, department stores, airports, and even in our own homes. In health care, bar-coding technology has been employed in areas such as materials management, supply inventory, and document management. However, medication administration using BPOC, which has the potential to enhance productivity, improve patient safety, and ultimately, improve quality of care, is a new area of emphasis for this technology (Low & Belcher, 2002). To be effective, medication administration BPOC systems must be combined with decision-support capabilities and enable alerts and warnings designed to prevent errors. The goal is to ensure that the system identifies the right patient for the right treatment at the right time.

Most medication administration BPOC systems operate in essentially the same way. At the time of admission the patient receives an identification wristband with a bar code. This wristband correctly identifies the patient by name, date of birth, medical record number, and any other important identifying information. Correctly identifying the patient is the first step in seeing that the right patient gets the right medication. Next the provider scans his or her own bar-coded identification band in order to log into the medication administration system. Bar-coding the provider or employee gives positive identification of the caregiver and ensures secure access to various information systems, according to the individual user's privileges. It also provides an audit trail of who has accessed what systems at what time and for what information. When the provider scans the patient's bar-coded wristband, he or she has access to the physician's orders and can view what currently needs to be done for the patient. When the caregiver scans a bar-coded item or medication, that code is compared with the order profile. If it does not match, the caregiver is alerted to the discrepancy, and a potential error is averted. The scanning process might also trigger real-time documentation and billing.

Studies have shown that about half of medication errors occur during the ordering process (Hatoum, Catizone, Hutchinson, & Purohit, 1986; Jenkins & Bond, 1996; Lesar, Briceland, & Stein, 1997), but errors also occur in dispensing, administering, and monitoring medications (Kaushal & Bates, 2002). Medication administration systems

that use BPOC can be highly effective in reducing all types of medication errors, wherever in the treatment cycle they occur; yet only 1.1 percent of U.S. hospitals have bedside scanners (Barlas, 2002).

To aid health care organizations in implementing BPOC, HIMSS (2003b) has developed a resource guide that outlines how bar coding works, describes clinical and administrative applications that can employ bar-coding technology, and offers strategies and tips for successfully implementing bar coding in health care organizations. For example, the guide points out that only about 35 percent of medications come from the manufacturer with bar-coded labels, so health care organizations planning to employ BPOC systems need to have their pharmacies apply bar-coded labels or arrange for these labels to be applied by a repackager (HIMSS, 2003b, p. 11).

Telemedicine

Telemedicine is the use of telecommunications for the clinical care of patients, and it may involve various electronic delivery mechanisms. It is a tool that enables providers to deliver health care services to patients at distant locations. Telemedicine systems have evolved over the past few decades, becoming most prevalent during the 1990s owing to major advancements in telecommunications technology and decreases in equipment and transmission costs. Telemedicine may be as simple as two health care providers discussing a case over the telephone or as sophisticated as using satellite technology and videoconferencing equipment to broadcast a consultation between providers at facilities in two countries. The first method is used daily by most health professionals, and the second is used by the military and some large medical centers.

Health care literature often uses the terms *telemedicine* and *telehealth* interchangeably. The term *telehealth* was originally used to describe administrative or educational functions related to telemedicine. According to Brown (2002), the term *telehealth* has emerged recently as an umbrella term for the wide range of uses of telecommunications to deliver health care services. Physicians and their patients using e-mail communication or patients using Internet-based services to fill drug prescriptions and obtain other health services are examples of telehealth. The term *telemedicine* more commonly refers to the direct provision of clinical care via telecommunications—diagnosing, treating, or following up with a patient at a distance (Brown, 2002). We will follow this distinction in describing the general use and acceptance of telemedicine and telehealth programs.

Current Status of Telemedicine Programs. There are currently over 200 telemedicine programs throughout the United States and abroad (Brown, 2004). Many of these were established at academic medical centers or initially funded as pilot projects in rural or medically underserved areas. For instance, the University of Kansas has used

telemedicine for several years to provide clinical services to oncology patients and mental health services to patients in rural correctional facilities (University of Kansas Medical Center, 2004). It has also used telemedicine to augment school health services by giving school nurses the opportunity to consult with physicians. Like the program at the University of Kansas, the telemedicine program at the University of Texas Medical Branch (UTMB) at Galveston also serves patients in correctional institutions (UTMB, 2004). In fact, it was one of the first telemedicine programs in the country to provide services to inmates, and it currently serves approximately 400 patients a month. The UTMB saw telemedicine as a means of decreasing the costs and dangers associated with transporting prisoners to health care facilities. Other organizations use telemedicine technology to deliver home health, mental health, radiology, and dermatology services to individuals living in rural or underserved communities (Brown, 2004).

Primary Delivery Methods. There are two primary means of delivering telemedicine services or technology. The first is called *store and forward*. This technology is used primarily for transferring digital images from one location to another. For example, a digital image might be taken with a digital camera, *stored* on a server, and then sent (or *forwarded*) to a health care provider at another location upon request (Brown, 2002). Teleradiology and teledermatology are two telemedicine services that use store-and-forward technology. In the case of teleradiology, one provider might send radiological images such as X-rays, CT scans, or magnetic resonance images (MRIs), to another provider to review. In the case of teledermatology, a digital image of the patient's skin might be sent to a dermatologist for diagnosis or consultation. Store-and-forward technology is generally used in nonemergency situations.

The second major type of telemedicine technology is known as *two-way interactive television* (IATV) and is used when a face-to-face consultation is necessary (Brown, 2002). For example, the patient and a provider at one location might consult with a specialist in another location using real-time videoconferencing capabilities. IATV gives patients and providers living in rural communities access to providers, particularly specialists, in urban areas without having to travel. In addition, a number of peripheral devices can be linked to computers to aid in interactive examination. For example, a stethoscope can be linked to a computer, allowing the consulting physician to hear the patient's heartbeat from a distance.

The military and some university research centers are also developing robotic equipment for *telesurgery* applications. Telesurgery might enable a surgeon in one location to remotely control a robotic arm to perform surgery in another location. The military has developed this technology particularly for battlefield use, although some academic medical centers are also piloting telesurgery technology.

Value of Telemedicine. Telemedicine can make specialty care more accessible to rural and medically underserved communities. Through videoconferencing, a patient or provider living in a rural community can consult with specialists living at a distance, and this can reduce or eliminate travel and other costs associated with delivering health care services. An unpublished study of teler dermatology services at Partners HealthCare System in 2001 found that dermatologists were at least three times as efficient when providing teleconsultation services as they were when treating patients in their traditional offices. Patients also reported that they achieved symptom relief twice as fast with the teler dermatology consult and were very comfortable with the teler dermatology process. Kaiser Permanente conducted a study examining the impact of remote video technology on quality, use, patient satisfaction, and cost savings in the home health care setting. It found that the technology was well received by patients, capable of maintaining quality of care, and had the potential for cost savings if used as a substitute for some in-person visits (Johnston, Wheeler, Deuser, & Sousa, 2000).

These are but two examples of the value of telemedicine. Remote surgery would be a third source of value. It could bring to local communities access to the top specialists in the world. The possibilities for the use of telemedicine are endless. However, there are several major barriers that must be addressed if telemedicine is to be more widely used and available. In today's environment its cost effectiveness has yet to be fully demonstrated.

Telehealth

In recent years patients have increasingly turned to the Internet to obtain health care information and seek health care services, and a growing number of them are interested in communicating with their physicians directly on line regarding specific health needs. Physicians, in contrast, have not adopted these tools as readily as patients would like. They fear that communicating by e-mail with patients will create more work, result in inadequate reimbursement for the increased work, and lead to an increase in liability, security, and patient privacy concerns (MacDonald, 2003).

Several studies have examined the use and impact of on-line communication, and specifically the use of electronic mail, between patients and their providers. In 2003, the California HealthCare Foundation reported on a study of the various methods that can be used to facilitate on-line communication between patient and provider (MacDonald, 2003). On-line patient-provider communication was defined as "the electronic exchange of information between the patient and member of his or her physician practice" (p. 6). On-line communication from a patient may be everything from requesting an appointment to viewing a bill to requesting refills on prescriptions to seeking advice or a consultation via e-mail. Our discussion focuses on the use of e-mail between patients and their providers because it tends to be the most controversial and debated issue.

Current Use of E-Mail Communication Between Physicians and Patients. Approximately 25 percent of physicians use e-mail to communicate with their patients, according to a Deloitte Research Survey (Miller, Hillman, & Given, 2004). This rate compares to approximately 90 percent of American adults with Internet access who would like to communicate with their physicians via e-mail (Taylor & Leitman, 2002).

E-mail communication between physicians and patients has been used for a variety of purposes, including follow-up patient care, clarification on advice, prescription refills, and patient education. In one of the largest studies to date on the use of e-mail between physicians and patients, researchers at the University of Michigan Health System found that physicians were most amenable to e-mail communication with patients when a triage system was in place (MacDonald, 2003). The participating physicians wanted nurses and other staff members to first sort the messages and pass on only those messages that warranted a physician's response. The researchers also found that although the e-mail system improved communication between physicians and patients, it also increased the workload for physician practices.

Value of E-Mail Communication Systems. Physicians who e-mail their patients say that it allows them to leave direct responses to a patient's questions at the physicians' convenience. Many physicians complain of playing "telephone tag" with their patients and having to leave messages on patients' answering machines. MacDonald (2003) found a number of advantages for both the patient and the provider in using e-mail communication. E-mail

- Is asynchronous (no telephone tag). A provider can respond to many patient questions at the provider's convenience and therefore is not interrupting other patients' office visits to answer phone requests.
- Decreases telephone hold times.
- Is legible. An e-mail message clearly identifies the patient and enables the patient to communicate in his or her own words, without the risk that the message will be miscommunicated by an intermediary. Likewise, because the messages are typed, they are more legible than handwritten notes from office staff.
- Can automatically document a conversation. Many information systems record e-mail communications directly into the patient's medical record.
- Does not increase physicians' workload or decrease their productivity.
- Reduces patient visits and telephone calls.
- Reduces administrative tasks. A pilot project conducted by ConnectiCare, a Connecticut-based payer, found that e-mail communication increased productivity of physicians by reducing administrative tasks ("Connecticut Health Plan to Expand Online Physician Consultation Program," 2002).
- Allows more uninterrupted time for patients during office visits.

Despite these advantages, many issues need to be addressed if on-line communication between patients and their providers is to become widespread. Research shows that at least six critical considerations should be addressed when instituting an e-mail communication system between patients and providers (MacDonald, 2003):

1. *Complexity of infrastructure.* The complexity of the technical infrastructure needed to support on-line patient-provider communication tools can vary. It runs the gamut from simple stand-alone products that are easy to install and maintain to EMR systems with integrated communication tools that document all correspondence in the patient's medical record.
2. *Degree of integration.* Similarly, electronic messaging can either stand alone or be well integrated into an existing system such as an EMR. Messaging systems integrated into an existing EMR typically record each e-mail communication as part of the patient's medical record.
3. *Message structure.* On-line messages may be structured or unstructured. Many messaging tools use templates or forms to guide and limit the information that is provided to physicians or other providers. Other tools allow patients to send e-mail messages comparable to those they might send a friend or colleague. They can ask any question on any topic at any length. Structured and unstructured messages will be handled differently, affecting the organization's workflow. For example, a patient requesting a prescription refill in a structured message can be required to pick from a list of his or her current medications, reducing the likelihood that someone will misunderstand which medication the patient wants. In addition the receiving computer will be able to recognize the message as a prescription request and route it to the appropriate person.
4. *Cost.* The cost of on-line communication tools can vary considerably. The stand-alone systems tend to be less expensive and require less upfront capital compared to integrated systems.
5. *Security.* Patient privacy should be of utmost concern, and therefore it is critical that e-mail messages exchanged over the Internet be encrypted. Encryption requires special software that scrambles the message and permits only authorized readers to unscramble and read it.
6. *Reimbursement.* Many physicians are concerned that they will not be adequately compensated for the time they spend communicating electronically with patients. The methods that have been explored to compensate physicians for their time include (a) reimbursement by payers on a per message basis; (b) reimbursement by patients on a per message basis; and (c) reimbursement by patients on an annual basis.

When a health care organization opts to institute e-mail communication between patients and clinicians or among clinicians, it should not only address these six elements but also establish policies and guidelines for appropriate system use. The American

Medical Association (2003) has published guidelines for on-line communication that health care organizations about to embark on such an initiative can use as a resource. Figure 5.8 presents an example of an e-mail communication policy developed by an integrated health care network.

Fitting Applications Together: The EMR Is the Hub

How are the clinical information systems or applications discussed in this chapter related? How can they fit together? We view the patient's electronic medical record as the *hub* of all the clinical information gathered by a health care organization (Figure 5.9). The data that eventually make up each patient's record originate from a variety of sources—both paper and electronic. In an electronic environment the data are typically captured by a host of different applications, including but not limited to

- *Admissions or registration systems*: patient demographic information, health insurance or payer, provider's name, date and reason for visit or encounter, and so forth
- *Accounting systems*: patient billing information such as final diagnosis and procedure codes, charges, dates of services provided, and so forth
- *Ancillary clinical (laboratory, radiology) systems*: diagnostic tests, therapeutic procedures, results, and so forth
- *CPOE systems*: physician orders, date, time and status, and so forth
- *Medication administration systems*: medications ordered, dispensed, and administered, and so forth
- *Other clinical and administrative systems*: nursing, physical therapy, and nutrition education documentation; scheduling information; and so forth
- *Knowledge-based reference systems*: access to MEDLINE, the latest research findings, practice guidelines, and so forth
- *Telemedicine and telehealth systems*: documentation of provision of health care services, on-line communication with patients and providers, and so forth

Sometimes these applications are all components of a single vendor package. More commonly, however, especially in larger facilities, these applications have been acquired or developed over the past twenty to thirty years. The challenge many health care organizations now face is how to bring the patient's clinical and administrative data together—how to make all the systems containing these data function as a single, seamless, integrated application. If the goal of the electronic health record (EHR) is to be realized—that is, the capturing of patient information throughout the patient's lifetime and the sharing of health information among different organizations—we must begin developing organizational EMR systems.

FIGURE 5.8. SAMPLE E-MAIL COMMUNICATION POLICY.

GUIDELINES FOR CLINICAL ELECTRONIC MAIL COMMUNICATION

The following guidelines should be universally applied when using electronic mail (e-mail) to communicate patient-identifiable information. Electronic mail is vulnerable to access by many individuals. Such access includes but is not limited to messages sent to the correct person and read by the wrong person (for example, family member of patient, employer of the patient, or someone at the physician's office other than the physician who is responsible for the e-mail). Additionally, the contents of an e-mail may be altered without detection. *Many companies, including Partners and its entities, reserve the right to monitor their employees' e-mail messages to ensure that they are being used properly. Thus, it is possible that the patient's employer could read private messages.* These guidelines are recommended for e-mail communications that contain patient identifiable information.

E-Mail Guidelines Between Clinician and Patient

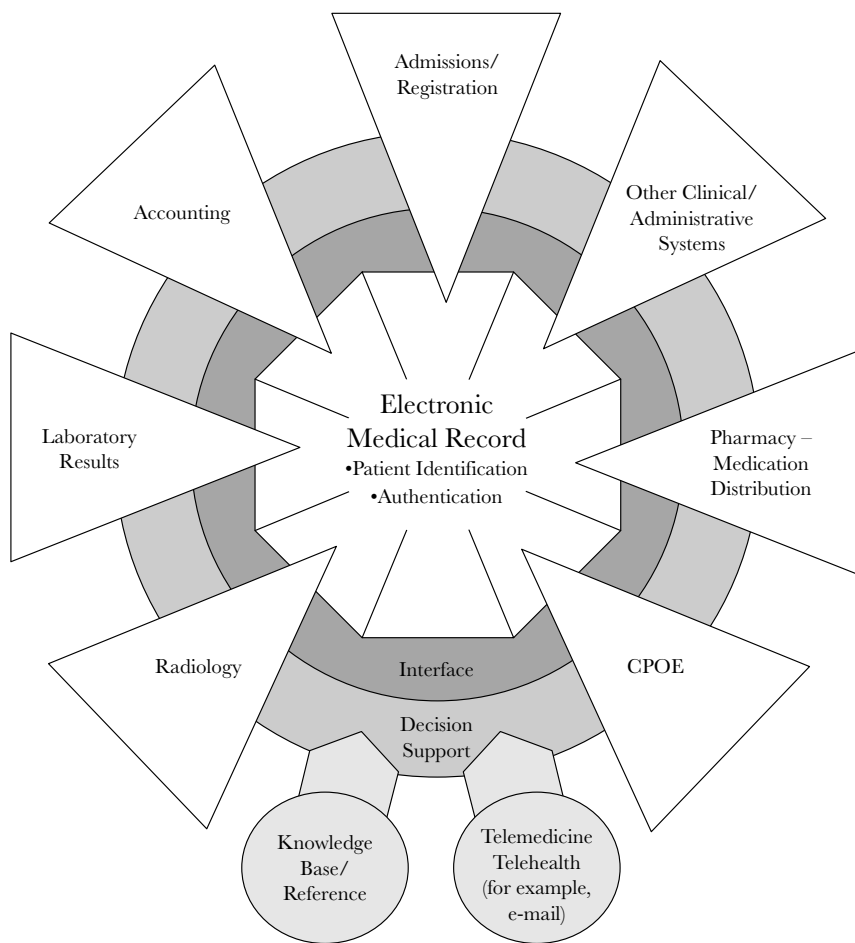
1. If a clinician and a patient agree to use electronic mail, patients should be informed about privacy issues. Patients should know that
 - Others besides the addressee may process messages during addressee's usual business hours, during addressee's vacation or illness, and so forth.
 - E-mail can occasionally be sent to the wrong party.
 - E-mail communication will not necessarily be a part of the patient's medical record.
 - E-mail can be accessed from various locations.
 - Information may be sent via e-mail to other care providers.
 - The Internet does not typically provide a secure media for transporting confidential information unless both parties are using encryption technologies.
 - Automatic forwarding of e-mail is allowed within the harvard.edu and Partners.org community. Messages can, however, be "forwarded" to another recipient at the sender's discretion.
2. Clinical interactions conducted by e-mail that a clinician believes should be part of the medical record should be stored in the patient's electronic or paper medical record.
3. If the patient's health information/treatment includes particularly sensitive information, ask the patient to decide whether this information may be referenced in e-mail, or should not be shared. Such information might include references to HIV status, substance abuse, sexually transmitted diseases, sexual assault, cancer, abortion, domestic violence, or confidential details of treatment with a psychotherapist, psychologist, or social worker. Until the patient's preference is known, content of this kind in an e-mail should be avoided.
4. Patients should be asked to write the category of transaction, for example, status, appointment, in the subject line of a message so that clinicians can more easily sort and prioritize their e-mails.
5. When available, clinicians and patients should use encryption technology for transmitting patient-identifiable information. Judgment should be used in the type of medical information that is transmitted, recognizing the increased vulnerability.

6. When possible, clinicians and patients should use a Read Receipt in order to acknowledge that they have read the message that was sent.
7. Patient-identifiable information should not be forwarded to a third party (nonclinician) without the patient's prior consent.

E-Mail Guidelines Between Clinicians

1. If clinicians agree to use e-mail to communicate patient-identifiable information between one another, both parties should be knowledgeable about privacy issues:
 - Others besides the addressee may process messages during addressee's usual business hours, during addressee's vacation or illness, and so forth.
 - E-mail can occasionally go to the wrong party.
 - E-mail communication will not necessarily be a part of the patient's medical record (see item 5 below).
 - E-mail can be accessed from various locations.
 - Information may be sent via e-mail to other care providers.
 - The Intranet provides a reasonable level of security.
 - The Internet does not typically provide a secure medium for transporting confidential information unless both parties are using encryption technologies.
2. The following statement should be added to each e-mail that leaves the Intranet:
"THE INFORMATION TRANSMITTED IN THIS E-MAIL IS INTENDED ONLY FOR THE PERSON OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN CONFIDENTIAL AND/OR PRIVILEGED MATERIAL. ANY REVIEW, RETRANSMISSION, DISSEMINATION OR OTHER USE OF OR TAKING OF ANY ACTION IN RELIANCE UPON, THIS INFORMATION BY PERSONS OR ENTITIES OTHER THAN THE INTENDED RECIPIENT IS PROHIBITED. IF YOU RECEIVED THIS E-MAIL IN ERROR, PLEASE CONTACT THE SENDER AND DELETE THE MATERIAL FROM ANY COMPUTER."
3. The category of transaction, for example, consult request, should be stated in the subject line of each e-mail message for clarification or filtering.
4. Changes should not be made to someone else's message and forwarded to others without making it clear where changes were made.
5. Discretion should be used when printing e-mail messages because printing all messages may defeat the purpose of e-mail (paperless medium) and may create confidentiality issues. However, clinical interactions conducted by e-mail that a clinician believes should be part of the medical record should be stored in the patient's electronic or paper medical record.

Source: Partners HealthCare System, Inc.

FIGURE 5.9. EMR: THE HUB OF CLINICAL INFORMATION SYSTEMS.

The primary mission of most health care organizations is to provide high-quality, cost-effective patient care. To this end many health care organizations are looking to provide practitioners with access to comprehensive health care information systems that will enable them to more effectively and efficiently care for patients. The acquisition of such systems does not generally occur at a specific moment in time but is a journey that occurs over many years. And despite the value and many benefits to be gained from adopting health care information systems, many organizations have yet to do so. A multitude of barriers must be overcome. In the next section we describe these major barriers, summarize some of the work already done to address them, and comment on the work still to do.

Barriers to Adoption

What do the EMR, EHR, CPOE, telemedicine, telehealth, and many other clinical applications all have in common? They all affect the ways providers deliver care to or communicate with patients, and they all confront the same barriers impeding their widespread adoption and use. Most of these barriers can be categorized as (1) financial, (2) organizational or behavioral, or (3) technical. Financial barriers include lack of the capital or other financial resources needed to develop, acquire, implement, and support a health care information system. Organizational and behavioral barriers relate to provider use and acceptance of such systems. And technical barriers include everything from the work needed to build system interfaces to a lack of adequate definitions and standards for data interchange. Although all three types of barriers typically affect all clinical applications, the actual impact of any one barrier may vary considerably across applications. For example, the lack of financial resources or of reimbursement for EMR systems has slowed their implementation but not stopped it. Conversely, the lack of financial resources or of reimbursement for telemedicine services has been devastating to telemedicine programs and many programs have not survived these financial difficulties.

Financial Barriers

EMR and related systems can be expensive to develop, implement, and support—and currently health care organizations are receiving little or no reimbursement for the improved care that can result from using them. The health care organization might invest a significant amount of money, personnel, and other resources in an EMR system and yet not realize a positive financial return on its investment (particularly at first), even if it realizes a return in terms of quality. This situation often makes it very difficult for health care executives to justify the EMR investment, especially in times when capital is tight.

The reimbursement concerns may be on the verge of decreasing, however. A number of studies are currently investigating the use of various financial incentives to encourage and reward health care organizations that use EMR-type systems. Here are five of the major current approaches (Mendelson, 2003):

1. *Payment differentials*: using bonuses or add-on payments that reward providers or delivery systems, or both, for adoption and diffusion of health care information systems that improve quality of care.
2. *Cost differentials*: using patient copayments or deductibles that vary by provider, based on predetermined quality measures. The intent is to steer patients to providers that have adopted health care information systems or achieved certain quality outcomes.

3. *Innovative reimbursement*: offering reimbursement for new categories of care or service that are directly related to the use of health care information systems (for example, the virtual provider-patient visit).
4. *Shared risk*: making a portion of provider fees or rate increases contingent on technology implementation or quality improvements.
5. *Combined programs*: combining two or more of the first four approaches, often with the included benefit of public disclosure of provider progress or outcomes.

Several of the major payers that are currently testing one or more of these reimbursement strategies are shown in Table 5.1. These strategies are attempts to find an answer to a fundamental question: Should a health plan pay for or reward providers or health care organizations that adopt health care information technology (such as EMR or CPOE systems), or should it pay for improvements in health outcomes? Or should it do both? It will be important to evaluate the success of these and other reimbursement strategies—and to ask such other important questions as

- Are these reimbursement efforts successful?
- Are these efforts replicable and sustainable?
- Are some efforts more successful than others, and why?
- Do some of these incentives have risk-averse consequences?
- What steps should be taken to facilitate broad implementation of these or other incentive programs?

Regardless of the reimbursement effort chosen, the incentives must be aligned with and must encourage the use of clinical information systems.

Telemedicine has faced financial barriers somewhat different from those encountered by other clinical systems. The initial telemedicine programs in the United States were grant-funded projects, and the majority of the funding came from the federal government. As federal funding for telemedicine has decreased in recent years, private corporations and telecommunications companies have sometimes stepped up to the plate in an attempt to keep these programs going (Brown, 2002). Yet the new funding has not been enough. Many telemedicine pilot programs have not endured beyond the life of their first funding. Again, the lack of reimbursement for telemedicine services has been a significant limiting factor. In 2003, federal legislation allowed health care organizations to be reimbursed by Medicare for professional consultations with specific clinicians via telecommunication systems when patients are seen at qualifying sites. However, store-and-forward technology is not a reimbursable service under the Medicare program, and reimbursement policies for Medicaid vary from state to state. Local third-party payers have individual practices for reimbursing for telemedicine services, and these practices vary across regions and states (American

TABLE 5.1. SOME CURRENT REIMBURSEMENT STRATEGIES.

Reimbursement Method	Programs
Payment differentials	Empire, Bridges to Excellence, MVP Health Plans/ Taconic IPA, IHA-PBGH, Blue Shield of CA, CMS, Group Health Cooperative
Shared risk	Harvard Pilgrim Health Care
Cost differentials	Hannaford Bros., Blue Shield of CA
Innovative reimbursement	ConnectiCare, Blue Shield of CA, Group Health Cooperative

Source: Mendelson, 2003.

Telemedicine Association, 2003). Until reimbursement issues are addressed at the federal, state, and local levels, the lack of funding for telemedicine applications will remain a major barrier to their widespread adoption and use.

Behavioral Barriers: Physician Acceptance

In addition to the financial barriers, many behavioral or organizational barriers impede the adoption of EMR systems and other clinical applications. These barriers can be equally as difficult to overcome as the financial barriers. They include everything from physician acceptance to changes in workflow to differences in state licensing regulations.

EMR and other clinical information systems may alter the way that providers interact with patients and render patient care services. They often require that providers directly enter visit notes, respond to system reminders and alerts, and give complete documentation. Studies have shown that EMR, CPOE, and other clinical information applications can be difficult to incorporate into existing workflow processes (Poon, Blumenthal, Jaggi, Honour, Bates, & Kaushal, 2004). When a system is initially implemented, it invariably adds time to the physician's day. This may seem contrary to one of the reasons for implementing EMR systems, to save time. In truth, EMR systems require that physicians respond to reminders, alerts, and other knowledge aids—all of which can lead to better patient care but may also require more time. For instance, suppose a physician is treating a patient with diabetes mellitus. The EMR might remind the physician to follow clinical practice guidelines for treating diabetes, which include conducting an eye exam and checking the patient's hemoglobin A1C levels—both of which take time. Without the EMR reminder, these tasks might have been forgotten. Unfortunately, most physicians receive no reimbursement or compensation for using EMR systems or for providing good-quality care. Until financial and reimbursement incentives are aligned with EMR use, physician acceptance will likely remain a critical barrier to system adoption.

This is not to say that all health care organizations have been unable to gain physician acceptance. Strong leadership support, initial and ongoing training, sufficient time to learn the intricacies of the system, and evidence that the system is well integrated with patient care workflow are all important factors in physician acceptance and use (Wager et al., 2000). Physicians need to realize the value that comes from using the clinical application—or they simply won't use it. The value could be improved patient services, improved quality of care, more highly satisfied patients, or happier staff or something more personal to the physician such as improved quality of documentation, less stress, and more leisure time. Factors leading to physician acceptance of clinical information systems will be discussed further in Chapter Seven.

When it comes to telemedicine and telehealth systems, things such as differences in state laws and in standard medical practice can affect physicians' attitudes and impede adoption. Many states will not permit out-of-state physicians to practice in their state unless licensed by them. Some physicians are concerned about medical liability issues and the lack of hands-on interaction with patients. Many physicians still prefer to meet with the patient and conduct the examination in person for fear of litigation or of missing important information.

Technical Barriers: Standards and Data Definitions

The third broad category of barriers to EMR-type systems involves technology; health care organizations must implement the technologies necessary to support and sustain these systems. They must choose these technologies wisely—understanding how emerging technologies fit with existing technologies, and engaging in continuing development and refinement of standards and data definitions.

Getting your arms around health care information standards is not an easy task. Many of the standards issues in health care also exist for the general business community; others are specific to health care. One thing is clear—standards are what enable different computer systems from different vendors and different health care organizations to share data. We discuss standards that affect health care information systems and how these standards are developed in greater detail in Chapter Nine. In the context of the present discussion, what is important to understand is that inadequate standards combined with rapidly changing technologies can be a barrier to widespread EMR adoption and use.

Health care organizations must also have a stable infrastructure to support clinical and administrative applications. The infrastructure must be reliable, fast, secure, and inexpensive. Failing to implement an adequate infrastructure can lead to poor system performance and insurmountable problems.

Summary

This chapter provided an overview of five emerging clinical information applications: EMR, CPOE, medication administration, telemedicine, and telehealth. We described each application and discussed its current use and its value to the patient, the provider, the health care organization, and the community at large. Special attention was given to the electronic medical record at the organizational level and the benefits it offers. These benefits include (1) improved quality, outcomes, and safety; (2) improved efficiency, productivity, and cost reductions; and (3) improved service and satisfaction. Despite the many benefits and advantages found in using EMR systems, the reality is that they are not widely used in health care today. The financial, behavioral, and technical barriers to their use were discussed, along with some of the strategies employed to overcome these barriers.

Chapter Five: Learning Activities

1. Search the Internet and find five health care information system vendors that offer EMR products. Compare and contrast the functions and features of each product. How do these systems compare with the MRI's and the IOM's definitions of the EMR?
2. Search the clinical management literature and find at least one article describing the adoption or use of (a) an EMR system, (b) a CPOE system, (c) a medication administration system using BPOC, (d) a telemedicine system, (e) telehealth system, or (f) other clinical information system or application. Summarize the article for your classmates, and discuss it with them. What are the key points of the article? What lessons learned does it describe?
3. Visit a health care organization that uses one of the clinical applications described in this chapter. Find out how the application's value is measured or assessed. What do providers think about it? Health care executives? Nurses? Support staff? What impact has it had on patient care?
4. Investigate what efforts are being made nationally and in your state (in both the public and private sectors) to further the adoption of EMR systems. How likely are these efforts to work? What concerns do you have about them? What else do you think is needed to further the adoption of EMR systems?



CHAPTER SIX

SYSTEM ACQUISITION

By now you should have an understanding of the various types of health care information systems and the value they can bring to health care organizations and the patients they serve. This chapter describes the typical process a health care organization goes through in acquiring or selecting a new clinical or administrative application. Acquiring an information system application can be an enormous investment for health care organizations. Besides the initial cost, there are a host of long-term costs associated with maintaining, supporting, and enhancing the system. Health care professionals need access to reliable, complete, and accurate information in order to provide effective and efficient health care services and to achieve the strategic goals of the organization. Selecting the *right* application, one that meets the organization's needs, is a critical step. Too often information systems are acquired without exploring all options, without evaluating costs and benefits, and without gaining sufficient input from key constituent user groups. The results can be disastrous.

This chapter describes the people who should be involved, the activities that should occur, and the questions that should be addressed in acquiring any new information system. The suggested methods are based on the authors' years of experience and countless case studies of system acquisition successes and failures published in the health care literature.

System Acquisition: A Definition

In this book *system acquisition* refers to the process that occurs from the time the decision is made to select a new system (or replace an existing system) until the time a contract has been negotiated and signed. System implementation is a separate process described in the next chapter. The actual system selection, or acquisition, process can take anywhere from a few days to a couple of years depending on the organization's size, structure, complexity, and needs. Factors such as whether the system is deemed a priority and whether adequate resources (time, people, and funds) are available can also directly affect the time and methods used to acquire a new system (McDowell, Wahl, & Michelson, 2003).

Prior to arriving at the decision to select a new system, the health care executive team should engage in a strategic information system planning process, in which the strategic goals of the organization are formulated and the ways in which information technology (IT) will be employed to aid the organization in achieving its strategic goals and objectives are discussed. We discuss the need for aligning the IT plans with the strategic goals of the organization and determining IT priorities in Chapter Twelve. In this chapter, we assume that a strategic IT plan exists, IT priorities have been established, the new system has been adequately budgeted, and the organization is ready to move forward with the selection process.

The System Acquisition Process: Scenario and Approaches

To gain an understanding of and appreciation for the activities that occur during system acquisition process, we will follow a health care facility through the selection process for a new information system—specifically, an electronic medical record (EMR) system. In this case the organization, which we will call Valley Practice, is a multi-physician primary care practice.

What process should the practice use to select the EMR? Should it purchase a system from a vendor, contract with an application service provider, or seek the assistance of a system developer? Who should lead the effort? Who should be involved in the process? What EMR products are available on the market? How reputable are the vendors who develop these products? These are just a few of the many questions that should be asked in selecting a new information system.

Although the time and the resources needed to select an EMR (or any health care information system) may vary considerably from one setting to another, some fundamental issues should be addressed in any system acquisition initiative. The sections

that follow the scenario describe in more detail the major activities that should occur (Figure 6.1), relating them to the multiphysician practice scenario. We assume that the practice wishes to purchase (rather than develop) an EMR system. However, we briefly describe other options and point out how the process may differ when the EMR acquisition process occurs in a larger health care setting, such as a hospital.

Perspective: Acquiring an EMR System

Valley Practice provides patient care services at three locations, all within a fifteen-mile radius, and serves nearly 100,000 patients. Valley Practice is owned and operated by seven physicians; each physician has an equal partnership. In addition to the physicians the practice employs nine nurses, fifteen support staff, a business officer manager, an accountant, and a chief executive officer (CEO).

During a two-day strategic planning session, the physicians and management team created a mission, vision, and set of strategic goals for Valley Practice. The mission of the facility is to serve as the primary care “home” of individuals within the community, regardless of the patients’ ability to pay. Valley Practice wishes to be recognized as a “high-tech, high-touch” practice that provides high-quality, cost-effective patient care using evidence-based standards of care. Consistent with its mission, one of the practice’s strategic goals is to replace its current paper-based medical record with an electronic medical record (EMR) system. Such a system should enable providers to care for patients using up-to-date, complete, accurate information, anywhere, anytime.

Dr. John Marcus, the lead physician at Valley Practice, asked Dr. Julie Brown, the newest partner in the group, to lead the EMR project initiative. Dr. Brown joined the practice two years ago after completing an internal medicine residency at an academic medical center that had a fully integrated EMR system available in both the hospital and its ambulatory care clinics. Of all the physicians at Valley Practice, Dr. Brown has had the most experience using an EMR. She has been a vocal advocate for implementing an EMR and believes it is essential to enabling the facility to achieve its strategic goals.

Dr. Brown agreed to chair the project steering committee. She invited other key individuals to serve on the committee, including Dr. Renee Ward, a senior physician in the practice; Mr. James Rowls, the CEO; Ms. Mary Matthews, RN, a nurse; and Ms. Sandy Raymond, the business officer manager. Dr. Brown suggested that the committee contract with a health care IT consultant to guide them through the system acquisition process. The physician partners approved this request, and the committee retained the services of Ms. Sheila Moore, a consultant with HIT Consulting Solutions, who came highly recommended by a colleague of Dr. Marcus’s.

After the project steering committee was formed, Dr. Marcus met with the committee to outline its charge and deliverables. Dr. Marcus expressed his appreciation to Dr. Brown and all of the members of the committee for their willingness to participate in this important initiative. He assured them that they had his full support and the support of the entire physician team.

FIGURE 6.1. OVERVIEW OF SYSTEM ACQUISITION PROCESS.

- Establish project steering committee and appoint project manager
 - Define project objectives and scope of analysis
 - Screen the marketplace and review vendor profiles
 - Determine system goals
 - Determine and prioritize system requirements
 - Develop and distribute a Request for Proposal (RFP) or a Request for Information (RFI)
 - Explore other options for acquiring system
 - Application service provider
 - Contract with system developer or build in-house
 - Evaluate vendor proposals
 - Develop evaluation criteria
 - Hold vendor demonstrations
 - Make site visits and check references
 - Prepare vendor analysis
 - Conduct cost-benefit analysis
 - Prepare summary report and recommendations
 - Conduct contract negotiations
-

Dr. Marcus reviewed with the committee the mission, vision, and strategic goals of the practice as well as the committee's charge. The committee was asked to fully investigate and recommend the top three EMR products available in the vendor community. He stressed his desire that the committee members would focus on EMR vendors that have experience and a solid track record in implementing systems in physician practices similar to theirs.

Dr. Marcus felt strongly that the EMR system needed to enable providers to access patient information from any of Valley Practice's three sites and from their homes. He also spoke of the need for the system to provide health maintenance reminders, drug interactions, and access to clinical practice guidelines or standards of care. One goal was to eventually rid Valley Practice of paper records and significantly decrease the amount of dictation and transcription currently being done. Dr. Ward, Mr. Rowls, and Ms. Matthews assumed leadership roles in verifying and prioritizing the requirements expressed by the various user groups.

Under the leadership of Dr. Brown the members of the project steering committee established five project goals and the methods they would use to guide their activities. Ms. Moore, the consultant, assisted them in clearly defining these goals and discussing the various options for moving forward. They agreed to consider EMR products from only those vendors that had five or more years of experience in the industry and had a solid track record of implementations (which they defined as twenty-five or more).

The five project goals were based on Valley Practice's strategic goals. These project goals were circulated for discussion and approved by the CEO and the physician partners. Once the goals were agreed upon, the project steering committee appointed a small task group of committee members to carry out the process of defining system functionality and requirements. Because staff time was limited, the task group conducted three separate focus groups during the lunch period—one with the nurses, one with the support staff, and a third with the physicians. Ms. Moore, the consultant, conducted the focus groups, using a semistructured nominal group technique.

Concurrently with the requirements definition phase of the project, Mr. Rowls and Dr. Brown, with assistance from Ms. Moore, screened the EMR vendor marketplace. They reviewed the literature, consulted with colleagues in the state medical association, and surveyed practices in the state that they knew used an EMR system. Mr. Rowls made a few phone calls to CIOs in surrounding hospitals who had experience with ambulatory care EMRs to get their advice. This initial screening resulted in the identification of eight EMR vendors whose products and services seemed to meet Valley Practice's needs.

Given the fairly manageable number of vendors, Ms. Moore suggested that the project steering committee use a short-form request for proposal (RFP). This form had been developed by her consulting firm and had been used successfully by other physician practices to identify top contenders. The short-form RFPs were sent to the eight vendors; six responded. Each of these six presented an initial demonstration of its EMR system on site. Following the demonstrations, the practice staff members completed evaluation forms and ranked the various vendors. After reviewing the completed RFPs and getting feedback on the vendor presentations, the committee determined that three vendors had risen to the top of the list.

Dr. Brown and Dr. Ward visited four physician practices that used EMR systems from these three finalists. Mr. Rowls checked references and prepared the final vendor analysis. A detailed cost-benefit analysis was conducted, and the three vendors were ranked. All three vendors, in rank order, were presented in the final report given to Dr. Marcus and the other physician partners.

Dr. Marcus, Dr. Brown, and Mr. Rowls spent four weeks negotiating a contract with the top contender. It was finalized and approved after legal review and after all the partners agreed to it.

Establish a Project Steering Committee

One of the first steps in any major project such as an EMR acquisition effort is to create a *project steering committee*. This committee's primary function is to plan, organize, coordinate, and manage all aspects of the acquisition process. Appointing a project manager with strong communication skills, organizational skills, and leadership abilities is critical to the project. In our Valley Practice case the project manager was a physician partner. In larger health care organizations such as hospitals, where a CIO is employed, the CIO would likely be involved in the effort and might also be asked to lead it.

Increasingly, clinicians such as physicians and nurses with training in informatics are being called on to lead clinical system acquisition and implementation projects. Known as *chief medical informatics officers* or *nursing informatics officers*, these individuals bring to the project a clinical perspective as well as an understanding of IT and information management processes. Regardless of the discipline or background of the project manager (for example, IT, clinical, or administrative), he or she should bring to the project passion, interest, time, and project management skills and should be someone who is well respected by the organization's leadership team and who has the political clout to lead the effort effectively.

Pulling together a strong team of individuals to serve on the project steering committee is also important. These individuals should include representatives from key constituent groups in the practice. At Valley Practice, a physician partner, a nurse, the business officer manager, and the CEO agreed to serve on the committee. Gaining project buy-in from the various user groups should begin early. This is a key reason for inviting representatives from key constituent groups to serve on the project steering committee. They should be individuals who will use the EMR system directly or whose jobs will be affected by it.

Consideration should also be given to the size of the committee; typically, having five to six members is ideal. In a large facility, however, this may not be possible. The committee for a hospital might have fifteen to twenty members, with representatives from key clinical areas such as laboratory medicine, pharmacy, and radiology in addition to representatives from the administrative, IT, nursing, and medical staffs.

It is important to have someone knowledgeable about IT serving on the project steering committee. This may be a physician, a nurse, the CEO, or an outside consultant. In a physician group practice such as Valley Practice, having an in-house IT professional is rare. The committee chair might look internally to see if someone has the requisite IT knowledge, skills, and interests and also the time to devote to the project, but also might look externally for a health care IT professional who might serve in a consultative role and help the committee direct its activities appropriately.

Define Project Objectives and Scope of Analysis

Once the project steering committee has been established, its first order of business is to clarify the charge to the committee and to define *project* goals. The *charge* describes the scope and nature of the committee's activities. The charge usually comes from senior leadership or a lead physician in the practice. Project goals should also be established and communicated in well-defined, measurable terms. What does the committee expect to achieve? What process will be used to ensure the committee's success? How will milestones be acknowledged? How will the committee communicate progress and resolve problems? What resources (such as time, personnel, and travel expenses) will

the committee need to carry out its charge? What method will be used to evaluate system options? Will the committee consider contracting with a system developer to build a system or outsourcing the system to an application service provider? Or is the committee only considering systems available for purchase from a health care information systems vendor?

Once project goals are formulated, they can guide the committee's activities and also clarify the resources needed and the likely completion date for the project. Here are some examples of typical project goals:

- Assess the practice's information management needs, and establish goals and objectives for the new system based on these needs.
- Conduct a review of the literature on EMR products and the market resources for these products.
- Investigate the top ten EMR system vendors for the health care industry.
- Visit two to four health care organizations similar to ours that have implemented an EMR system.
- Schedule vendor demonstrations for times when physicians, nurses, and others can observe and evaluate without interruptions.

As part of the goal-setting process, the committee should determine the extent to which various options will be explored. For example, the Valley Practice project steering committee decided at the onset that it was going to consider only EMR products available in the vendor community. The committee further stipulated that it would consider only vendors with experience (for example, five or more years in the industry) and those with a solid track record of system installations (for example, twenty-five or more installations). The committee members felt the practice should contract with a system developer only if they were unable to find a suitable product from the vendor community—their rationale being that the practice wanted to be known as high-tech, high-touch. They also believed it was important to invest in IT personnel who could customize the application to meet practice needs and would be able to assist the practice in achieving project and practice goals.

Screen the Marketplace and Review Vendor Profiles

Concurrently with the establishment of project goals, the project steering committee should conduct its first, cursory review of the EMR marketplace and begin investigating vendor profiles. Many resources are available to aid the committee in this effort. For example, the Valley Practice committee might obtain copies of recent market analysis reports—from research firms such as Gartner or KLAS—listing and describing the vendors that provide EMR systems for ambulatory care facilities. The committee

might also attend trade shows at professional association conferences such as the Healthcare Information and Management Systems Society (HIMSS) and the American Medical Informatics Association (AMIA). (Appendix A provides an overview of the health care IT industry and describes a variety of resources available to health care organizations interested in learning about health care IT products, such as EMR systems, available in the vendor community.)

Determine System Goals

Besides identifying project goals, the project steering committee should define *system* goals. System goals can be derived by answering questions such as: What does the organization hope to accomplish by implementing an EMR system? What is it looking for in a system? If the organization intends to transform existing care processes, can the system support the new processes? Such goals often emerge during the initial strategic planning process when the decision is made to move forward with the selection of the new system. At this point, however, the committee should state its goals and needs for a new EMR system in clearly defined, specific, and measurable terms. For example, a system goal such as “select a new EMR system” is very broad and not specific. Here are some examples of specific and measurable goals for a physician practice.

Our EMR System Should . . .

- Enable the practice to provide service to patients using evidence-based standards of care.
- Aid the practice in monitoring the quality and costs of care provided to the patients served.
- Provide clinicians with access to accurate, complete, relevant patient information, on site and remotely.
- Improve staff efficiency and effectiveness.

These are just a few of the types of system goals the project steering committee might establish as it investigates a new EMR for the organization. The system goals should be aligned with the strategic goals of the organization and should serve as measures of success throughout the system acquisition process.

Determine and Prioritize System Requirements

Once the goals of the new system have been established, the project steering committee should begin to determine system requirements. These requirements may address everything from what information should be available to the provider at the point of care to how the information will be secured to what type of response time is expected.

The committee may use any of a variety of ways to identify system requirements. One approach is to have a subgroup of the committee conduct focus-group sessions or small-group interviews with the various user groups (physicians, nurses, billing personnel, and support staff). A second approach is to develop and administer a written survey, customized for each user group, asking individuals to identify their information needs in light of their job role or function. A third is to assign a representative from each specific area to obtain input from users in that area. For example, the nurse on the Valley Practice project steering committee might interview the other nurses, the business office manager might interview the support staff. System requirements may also emerge as the committee examines templates provided by consultants or peer institutions, looks at vendor demonstrations and sales material, or considers new regulatory requirements the organization must meet.

The committee may also use a combination of these or other approaches. At times, however, users do not know what they want or will need. Hence it can be extremely helpful to hold product demonstrations, meet with consultants, or visit sites already using EMR systems, so that those who will use or be affected by the EMR can see and hear what is possible. Whatever methods are chosen to seek users' information system needs, the end result should be a list of requirements and specifications that can be prioritized, or ranked. This ranking should directly reflect the specific strategic goals and circumstances of the organization.

The system requirements and priorities will eventually be shared with vendors or the system developer; therefore, it is important that they are clearly defined and presented in an organized, easy-to-understand format. For example, it may be helpful to organize the requirements into categories such as *software* (system functionality, software upgrades), *technical infrastructure* (hardware requirements, network specifications, backup, disaster recovery, security), and *training and support* (initial and ongoing training, technical support). These requirements will eventually become a major component of the request for proposal (RFP) submitted to vendors or other third parties (discussed further later in this chapter).

Here are some of the issues an actual physician practice found it should be considering:

Perspective: Identifying System Requirements

In 2000, Palmetto Physicians Primary Care in Charleston, South Carolina, implemented an EMR system throughout its practices. According to CEO Ron Piccione, practice members discovered that in addition to identifying functional requirements they needed to address the following questions:

- How will technology upgrades be handled?
 - Hardware and software upgrades
 - Service and response times
 - Pricing
 - Expandability of system
- Who are the qualified vendors?
 - Financial and organizational stability
 - Regional locations
 - Experiences in comparable installations
 - Reference checks
- What are the implications for IT design?
 - Storage space
 - Electrical requirements (power, shielding, ventilation)
 - Reassessing location of clinical functions
 - Present capacity
- What other operations are affected by this technology?
 - Human resources (recruitment and retention, education, training)
 - Information services
 - Physical plant
 - Medical staff
 - Patient safety and error reduction
 - Finance (bond rating, cost accounting, return on investment)

Ron Piccione, personal communication, April 11, 2004

Develop and Distribute the Request for Proposal or Request for Information

Once the organization has defined its system requirements, the next step in the acquisition process is to package these requirements into a structure that a third party can respond to, whether that third party be a development partner or a health information systems vendor. Many health care organizations package the requirements into a *request for proposal* (RFP). The RFP provides the vendor with a comprehensive list of system requirements, features, and functions and asks the vendor to indicate whether its product or service meets each need. Vendors responding to an RFP are also generally required to submit a detailed and binding price quotation for the applications and services being sought.

RFPs tend to be highly detailed and are therefore time consuming and costly to develop and complete. However, they provide the health care organization and each vendor with a comprehensive view of the system needed. Health care IT consultants can be extremely resourceful in assisting the organization with developing and packaging the

RFP. An RFP for a major health care information system acquisition generally contains the following information (sections marked with an asterisk [*] are completed by the vendor; the other sections are completed by the organization issuing the RFP):

- *Instructions for vendors.*
 - Proposal deadline and contact information: where and when the RFP is due; whom to contact should the vendor have questions.
 - Confidentiality statement and instructions: a statement that both the RFP and the responses provided by the vendor are confidential and are proprietary information.
 - Specific instructions for completing the RFP and any stipulations with which the vendor must comply in order to be considered.
- *Organization objectives:* type of system or application being sought; information management needs and plans.
- *Background of the organization.*
 - Overview of the facility: size, types of patient services, patient volume, staff composition, strategic goals of organization.
 - Application and technical inventory: current systems in use, hardware, software, network infrastructure.
- *System goals and requirements:* goals for the system and functional requirements (may be categorized as *mandatory* or *desirable* and listed in priority order). Typically this section includes application, technical, and integration requirements.
- *Vendor qualifications*:* general background of vendor, experience, number of installations, financial stability, list of current clients, standard contract, and implementation plan.
- *Proposed solutions*:* how vendor believes its product meets the goals and needs of the health care organization. Vendor may include case studies, results from system analysis projects, and other evidence of the benefits of its proposed solution.
- *Criteria for evaluating proposals:* how the health care organization will make its final decisions on product selection.
- *General contractual requirements*:* such as warranties, payment schedule, penalties for failure to meet schedules specified in contract, vendor responsibilities, and so forth.
- *Pricing and support*:* quote on cost of system, using standardized terms and forms.

RFPs are not the only means by which to solicit information from vendors. A second approach that is often used is the *request for information* (RFI). An RFI is considerably shorter than an RFP and less time consuming to develop and is designed to obtain basic information on the vendor's background, product description, and service capabilities. Some health care organizations send out an RFI before distributing the RFP,

in order to screen out vendors whose products or services are not consistent with the organization's needs. Rather than seeking a specific quotation on price as the RFP does, the RFI simply asks the vendor to provide its guidelines for calculating the purchase price (DeLuca & Enmark, 2002).

How does one decide whether to use an RFP, an RFI, both, or neither during the system acquisition process? Several factors should be considered. Although time consuming to develop, the RFP is useful in forcing a health care organization to define its system goals and requirements and prioritize its needs. The RFP also creates a structure for objectively evaluating vendor responses and provides a record of documentation throughout the acquisition process. System acquisition can be a highly political process; by using an RFP the organization can introduce a higher degree of objectivity into that process. RFPs are also useful data collection tools when the technology being selected is established and fully developed, when there is little variability between vendor products and services, when the organization has the time to fully evaluate all options, and when the organization needs strong contract protection from the selected vendor (DeLuca & Enmark, 2002).

There are also drawbacks to RFPs. Besides taking considerable time to develop and review, they can become cumbersome, so detail oriented that they lose their effectiveness. For instance, it is not unusual to receive three binders full of product and service information from one vendor. If ten vendors respond to an RFP (about five is ideal), the project steering committee may be overwhelmed and find it difficult to wade through and differentiate among vendor responses. Having too much information to summarize can be as crippling to a committee in its deliberations as having too little.

Therefore a scaled-back RFP or an RFI might be a desirable alternative. An RFI might be used when the health care organization is considering only a small group of vendors or products or when it is still in the exploratory stages and has not yet established its requirements. Some facilities use an even less formal process consisting primarily of site visits and system demonstrations.

Regardless of the tool(s) used, it is important for the health care organization to provide sufficient detail about its current structure, strategic IT goals, and future plans that the vendor can respond appropriately to its needs. Additionally, the RFP or RFI (or variation) should result in enough specific detail that the organization gets a good sense of the vendor—its services, history, vision, stability in the marketplace, and system or product functionality. The organization should be able to easily screen out vendors whose products are undeveloped or not yet fully tested (DeLuca & Enmark, 2002).

Explore Other Options for Acquiring System

In our Valley Practice case the physicians and staff opted to acquire an EMR system from the vendor community. Organizations like Valley Practice often turn to the market

for products that they will run on their own IT infrastructure. But there are times when they do not go to the market—they chose to leverage someone else's infrastructure (by contracting with an application service provider) or they build the application (by contracting with a system developer or using in-house staff).

Contract with an Application Service Provider. *Application service provider* (ASP) is a relatively new term for an old concept. An ASP is a company that deploys, hosts, and manages one or more software packages through centrally located servers, often on a fixed per use basis or on a subscription basis (Kelly & Legrow, 2000). Health care organizations may contract with an ASP to deliver a standard application via a network (such as the Internet) in exchange for lease payments (in the form of fixed monthly fees, for example). It's somewhat analogous to the option of purchasing or leasing a car. ASPs are the leasing option. They are similar in concept to the shared-systems option used by many hospitals in the 1960s and 1970s when they could not afford or did not have the IT staff available in-house to run and support software applications and hardware.

Why might a health care organization consider contracting with an ASP rather than purchasing an EMR (or other application) from a vendor? There are several reasons. First, the facility may not have the IT staff needed to run or support the desired system. Hiring qualified personnel at the salaries they demand may be difficult, and retaining them may be equally as challenging. Second, ASPs typically enable health care organizations to use clinical or administrative applications with fewer upfront costs and less capital. For a small physician practice, these financial arrangements can be particularly appealing. Because ASPs offer fixed monthly fees or fees based on usage, organizations are better able to predict costs. Third, by contracting with an ASP, the health care organization can focus on its core business and not get bogged down in IT support issues, although it may still have to deal with issues of system enhancements, user needs, and the selection of new systems. Other advantages to using ASPs are rapid deployment, 24/7 technical support, and the perception that one can easily switch from one ASP to another.

ASPs also have some disadvantages and limitations that the health care organization should consider in its deliberations. Although rapid deployment of the application can be a tremendous advantage to an organization, the downside is the fact that the application will likely be a standard, off-the-shelf product, with little if any customization. This means that the organization has to adapt or mold its operations to the application rather than tailoring the application to meet the operational needs of the organization. A second drawback deals with technical support. Although technical support is generally available from an ASP, it is unrealistic to think that the ASP's support personnel will have intimate knowledge of the organization and its operations. Frustrations can mount when one lacks in-house IT technical staff when and where

they are needed. System security and confidentiality of the patient information maintained by the ASP are paramount concerns. How the ASP will secure information should be clearly specified.

The health care executive considering whether contracting with an ASP is the best approach should thoroughly research the company and its products and consider factors such as company viability, target market, functionality, integration, implementation and training, help desk support, security, pricing, and service levels (Kelly & Legrow, 2000).

Contract with a System Developer or Build In-House. A second alternative to purchasing a system from a vendor is to contract with a developer to design a system for your organization. The developer may be employed in-house or by an outside firm. Working with a system developer can be a good option when the health care organization's needs are highly uncertain or unique and the products available on the market do not adequately meet these needs. Developing a new or innovative application can also give the organization a significant competitive advantage. The costs and time needed to develop the application can be significant, however. It is also important to consider the long-term costs. Should the developer leave, how difficult would it be to hire and retain someone to support and maintain the system? How will problems with the system be addressed? How will the application be upgraded? What long-term value will it bring the organization? These are a few of the many questions that should be addressed in considering this option. It is rare for a health care organization to develop its own major clinical information system.

Evaluate Vendor Proposals

In the Valley Practice case the project steering committee decided to focus its efforts at first on considering only EMR products available for purchase in the vendor community. The project steering committee came to this conclusion after its initial review of the EMR marketplace. Committee members felt there were a number of vendors whose products appeared to meet practice needs. They also felt strongly that in-house control of the EMR system was important to achieving the practice goal of becoming a high-tech, high-touch organization because they wanted to be able to customize the application. Realizing this, the committee had budgeted for an IT director and an IT support staff member. Members felt that the long-term cost savings from implementing an EMR would justify these two new positions.

Develop Evaluation Criteria. The project steering committee at Valley Practice decided to go through the RFP process. It developed criteria by which it would review and evaluate vendor proposals. Criteria were used to grade each vendor's response to the

RFP. Grading scales were established so the committee could accurately compare vendors' responses. These grading scales involved assigning more weight to required items and less weight to those deemed merely desirable. Categories of "does not meet requirement," "partially meets requirement," and "meets requirement" were also used. RFP documents were compared item-by-item and side-by-side, using the grading scales established by the committee (as in the example in Table 6.1). To avoid information overload, a common condition in the RFP review process, the project steering committee focused on direct responses to requirements and referred to supplemental information only as needed. Summary reports of each vendor's response to the RFP were then prepared by a small group of committee members and distributed to the committee at large.

Hold Vendor Demonstrations. During the vendor review process, it is important to host vendor system demonstrations. The purpose of these demonstrations is to give the members of the health care organization an opportunity to (1) evaluate the look and feel of the system from a user's point of view, (2) validate how much the vendor can deliver of what has been proposed, and (3) narrow the field of potential vendors (Superior Consultant Company, 2004). It is often a good idea to develop demonstration scripts and require all vendors to present their systems in accordance with these scripts. Scripts generally reflect the requirements outlined in the RFP and contain a moderate level of detail. For example, a script might require demonstrating the process of registering a patient or renewing a prescription. The use of scripts can ensure that all vendors are evaluated on the same basis or functionality. At the same time, it is important to allow vendors some creativity in presenting their product and services. When scripts are used, they need to be provided to vendors at least one month in advance of the demonstration, and both vendors and health care organization must adhere to them.

Criteria should be developed and used in evaluating vendor demonstrations, just as they are for reviewing vendor responses to the RFP.

Make Site Visits and Check References. After reviewing the vendors' RFPs and evaluating their product demonstrations, it is advisable to make site visits and check references. By visiting other facilities that use a vendor's products, the health care organization should gain additional insight into what the vendor would be like as a potential partner. It can be extremely beneficial to visit sites similar to your organization. For instance, in the Valley Practice case, representatives from key practice constituencies decided to visit other ambulatory care practices to see how a specific system was being used, the problems that had been encountered, and how these problems had been addressed.

How satisfied are the staff with the system? How responsive has the vendor been to problems? How quickly have problems been resolved? To what degree has the vendor delivered on its promises? Hearing answers to such questions firsthand from a variety of users can be extremely helpful in the vendor review process.

**TABLE 6.1. SAMPLE CRITERIA FOR EVALUATION
OF A VENDOR'S RFP RESPONSES.**

Type of Application: Electronic Medical Record System			
Vendor Name: The EMR Company	Meets Requirement	Partially Meets Requirement	Does Not Meet Requirement
Criteria:			
1. Alerts user to possible drug interactions	x		
2. Provides user with list of alternate drugs	x		
3. Advises user on dosage based on patient's weight	x		
4. Allows user to enter over-the-counter medications		x (on different screen)	
5. Allows easy print out of prescriptions	x		

Other Strategies for Evaluating Vendors. A host of other strategies can be used to evaluate a vendor's reputation and quality of product and service. One might attend vendor user-group conferences, review the latest market reports, consult with colleagues in the field, seek advice from consultants, and request an extensive list of system users.

Prepare Vendor Analysis. Throughout the vendor review process, the project steering committee members should have evaluation tools in place to document their impressions and the views of others in the organization who participate in any or all of the review activities (review of RFPs, system demonstrations, site visits, reference checks, and so forth). The committee should then prepare vendor analysis reports that summarize the major findings from each of the review activities. How do the vendors compare in reputation? In quality of their product? In quality of service? How do the systems compare in terms of their initial and ongoing costs? To what degree is the vendor's vision for product development aligned with the organization's strategic IT goals?

Conduct a Cost-Benefit Analysis

The final analysis should include an evaluation of the cost and benefits of each proposed system. The capital cost analysis may include software, hardware, network or infrastructure, third-party, and internal capital costs. The total cost of ownership should

factor in support costs and the costs of the resources needed (including personnel) to implement and support the system. Once the initial and ongoing costs are identified, it is important to weigh them against the benefits of the systems being considered. Can the benefits be quantified? Should they be included in the final analysis?

Prepare a Summary Report and Recommendations

Assuming the capital cost analysis supports the organization in moving forward with the project, the project steering committee should compile a final report that summarizes the process and results from each major activity or event. The report may include

- System goals and criteria
- Process used
- Results of each activity and conclusions
- Cost-benefit analysis
- Final recommendation and ranking of vendors

It is generally advisable to have two or three vendors in the final ranking, in the event that problems arise during contract negotiations, the final step in the system acquisition process.

Conduct Contract Negotiations

The final step of the system acquisition process is to negotiate a contract with the vendor. This too can be a time-consuming process, and therefore it is helpful to seek expert advice from business or legal advisers. The contract outlines expectations and performance requirements, who is responsible for what (for example training, interfaces, support), when the product is to be delivered (and vendor financial liability for failing to deliver on time), how much customization can be performed by the organization purchasing the system, how confidentiality of patient information will be handled, and when payment is due.

Project Management Tools

Throughout the course of the system acquisition project, a lot of materials will be generated, many of which should be maintained in a project repository. A *project repository* serves as a record of the project steering committee's progress and activities. It includes such information as minutes of meetings, correspondence with vendors, the request for proposal or request for information, evaluation forms, and summary reports. (Figure 6.2 lists the contents of a sample project repository.) This repository can be extremely

FIGURE 6.2. SAMPLE PROJECT REPOSITORY.

- Committee charge and membership (including contact information)
 - Project objectives (including method that will be used to select system)
 - System goals
 - Timeline of committee activities (for example, Gantt chart)
 - System requirements (mandatory, desirable)
 - Request for proposal
 - Request for information
 - Evaluation forms
 - Responses from RFPs
 - Vendor demonstrations
 - Site visits
 - Reference checks
 - Summary report and recommendations
 - Project budget and resources
-

useful when there are changes in staff or in the composition of the committee and when the organization is planning for future projects. The project manager should assume a leadership role in ensuring that the project repository is established and maintained.

Managing the various aspects of the project and coordinating activities can be a challenging task, particularly in large organizations or when a lot of people are involved and many activities are occurring simultaneously. It is important that the project manager helps those involved to establish clear roles and responsibilities for individual committee members, to set target dates, and to agree upon methods for communicating progress and problems. Many project management tools exist that can be useful here. For example, a simple Gantt chart (Figure 6.3) can document project objectives, tasks and activities, responsible parties, and target dates and milestones. A Gantt chart also gives a graphical representation of all project tasks and activities that shows which ones may occur simultaneously and which ones must be completed before another task can begin. Other tools enable one to allocate time, staff, and financial resources to each activity. Gantt charts or other timelines can be created with software programs such as Visio, Microsoft Project, or SmartDraw. A discussion of these tools is beyond the scope of this book but can be found in most introductory project management textbooks.

It is important to clearly communicate progress both within the project steering committee and to individuals outside the committee. Senior management should be kept apprised of project progress, budget needs, and committee activities. Regular updates should be provided to senior management as well as other user groups involved in the process. Communication can be both formal and informal—everything from periodic update reports at executive meetings to facility newsletter briefings to informal discussions at lunch.

FIGURE 6.3. SAMPLE GANTT CHART.

ID	EMR Selection Project	Start	End	Jan 2005		Feb 2005				Mar 2005					
				1/16	1/23	1/30	2/6	2/13	2/20	2/27	3/6	3/13	3/20		3/27
1	Define project objectives	1/17/2005	1/17/2005												
2	Conduct preliminary review of vendors	1/21/2005	2/8/2005												
3	Determine system requirements	1/21/2005	3/15/2005												
4	Conduct focus groups	2/1/2005	2/28/2005												
5	Survey key user groups	2/1/2005	3/10/2005												
6	Develop and administer RFP	3/15/2005	4/15/2005												
7	Hold vendor demonstrations	4/15/2005	4/29/2005												
8	Conduct cost-benefit analysis	5/2/2005	5/13/2005												

Things That Can Go Wrong During the System Acquisition Process

Managing the system acquisition process effectively requires strong and effective leadership, planning, organization, and communication skills. Things can and do go wrong. Upholding a high level of objectivity and fairness throughout the acquisition process is important to all parties involved. Failing to do so can dampen the overall success of the project. Following is a list of some common pitfalls in the system acquisition process, along with strategies for avoiding them.

- *Failure to manage vendor access to organization leadership.* The vendor may schedule private time with the CEO or a board member in the hope of influencing the decision and bypassing the project steering committee entirely. It is not unusual to hear that processes or decisions have been altered after the CEO has been on a golf outing or taken a trip to the Super Bowl with a vendor. The vendor may persuade the CEO or a board member to overturn or question the decisions of the project steering committee, crippling the decision process. Hence it should be clearly communicated to all parties (senior management, board, and vendor) that all vendor requests and communication should be channeled through the project steering committee.
- *Failure to keep the process objective (getting caught up in vendor razzle-dazzle).* Related to the need to manage vendor access to decision makers is the need to keep the process objective. The project steering committee should assume a leadership role in ensuring that there are clearly defined criteria and methods for selecting the vendor. These criteria and methods should be known to all the parties involved and should be adhered to. Additionally, it is important that the health care organization remain

unbiased and not get so impressed with the vendor's razzle-dazzle (in the form, for example, of exquisite dinners or fancy gadgets) that it fails to assess the vendor or the product objectively.

- *Overdoing or underdoing the RFP.* Striking a balance between too much and too little information and detail in the RFP and also determining how much weight to give to the vendors' responses to the RFP can be challenging. The project steering committee should err on the side of being reasonable—that is, the committee should include enough information and detail that the vendor can appropriately respond to the organization's needs and should give the vendor responses to the RFP appropriate consideration in the final decision. Organizations should also be careful that they do not assign either too much or too little weight to the RFP process.
- *Failure to involve the leadership team and users extensively during the selection process.* A sure way to disenchant the leadership team and end-users is to fail to involve them adequately in the system acquisition process. There should be ample opportunity for people at all levels of the organization who will use or be affected by the new information system to have input into its selection. Involvement can include everything from being invited and encouraged to attend vendor presentations during uninterrupted time to being asked to join a focus group where user input is sought. It is important that the project steering committee seek input and involvement throughout the acquisition process, not simply at the end when the decision is nearly final. Far too often information system projects fail because the leadership team and end-users were not actively involved in the selection of the new system.
- *Turning negotiations into a blood sport.* You want to negotiate a fair deal with the vendor and not leave the vendor's people feeling as though they have just been "beaten" in a contest. A lopsided deal results in a disenchanted partner and can create a bad climate. It is important to form a healthy, respectful, long-term relationship with the vendor.

These are just a few of the many issues that can arise during the system acquisition process that the health care executive should be aware of. Failing to appropriately address these issues can interfere with the organization's ability to successfully select and implement a system that will be adopted and widely used.

Summary

Acquiring or selecting a new clinical or administrative information system is a major undertaking for a health care organization. It is important that the process be managed effectively. Although the time and resources needed to select a new system will vary depending on the size, complexity, and needs of the organization, certain fundamental issues should be addressed in any system acquisition project.

This chapter discussed the various activities that occur in the system acquisition process. These activities were presented in the context of a multiphysician group practice that wishes to replace its current paper record with an EMR system by acquiring a system from a reputable vendor. Key activities in the system selection process are (1) establishing a project steering committee and appointing a strong project manager to lead the effort, (2) defining project objectives, (3) screening the vendor marketplace, (4) determining system goals, (5) establishing system requirements, (6) developing and administering a request for proposal or request for information, (7) evaluating vendor proposals, and (8) conducting a cost-benefit analysis on the various options. Other options such as contracting with an application service provider (ASP) or a system developer were also discussed. Finally, this chapter presented some of the issues that can arise during the system selection process and outlined the importance of documenting and communicating project activities and progress.

Chapter Six: Learning Activities

1. Interview a health care executive regarding the process last used by his or her organization to acquire a new information system. How did that process compare with the system acquisition process described in this chapter?
2. Assume you are part of a project steering committee in a rural nonprofit hospital. The hospital is interested in acquiring a new provider order entry system. You offer to screen the marketplace to see what types of computerized provider order entry systems are available. Prepare a fifteen-minute summary report of your findings to the committee at large.
3. Conduct a literature review (including an Internet search) to learn about application service provider organizations that offer EMR systems to physician practices. Briefly summarize the EMR products available from at least three different ASPs. What criteria might you use to compare them?
4. Find and critique a sample RFP for a health care organization. What did you like about it? What aspects of it did you feel could be improved? Explain.
5. This chapter described a typical physician practice that wishes to select an EMR system. Using the information in the Valley Practice scenario, draft a script for the vendors to use in describing their product and services. Include a description of the process you used to arrive at the script.
6. Working with your classmates (in small groups), assume that you are a Valley Practice committee member interested in obtaining user feedback on the EMR vendor demonstrations. Develop a survey instrument that might be used to solicit and summarize participants' responses to each vendor demonstration. Swap the survey your group designed with another group's survey; critique each other's work.



CHAPTER SEVEN

SYSTEM IMPLEMENTATION AND SUPPORT

Once a health care organization has finalized its contract with the vendor to acquire an information system, the system implementation process begins. Selecting the *right* system does not ensure user acceptance and success; the system must also be incorporated effectively into the day-to-day operations of the health care organization and adequately supported or maintained. Regardless of whether the system is built in-house, designed by an outside consultant, leased from an application service provider, or purchased from a vendor, a substantial amount of planning and work must occur to get the system up and running smoothly and integrated into operations.

This chapter describes the planning and activities that should occur when implementing a new system. Our discussion focuses on the activities associated with implementing a vendor-acquired system; however, many of these same activities apply to systems that are designed in-house, by an outside developer, or acquired through an application service provider.

Implementing a new system (or replacing an old system) can be a massive undertaking for a health care organization. Not only are there workstations to install, databases to build, and networks to test, but there are also processes to redesign, users to train, data to convert, procedures to write, and a host of behavioral and organizational issues to address. There are countless tasks and details that must be appropriately coordinated and completed if the system is to be implemented on time and within budget—and widely accepted by users.

Along with the activities, or tasks, that need to be undertaken during the technical implementation of a new information system, it is equally important to address organizational and behavioral issues. Studies have shown that over half of all information system projects fail. Numerous political, cultural, and behavioral factors can affect the successful implementation and use of the new system (Aarts, Doorewaard, & Berg, 2004; Berg, 2001). We devote a section of this chapter to the organizational and behavioral issues that can arise and things that can go wrong during the system implementation process and offer strategies for avoiding them. The chapter concludes by describing the importance of maintaining and supporting information systems.

System Implementation Process

System implementation begins once the organization has acquired the system and continues through the early stages following the *go-live* date (the date when the system is put into general use for everyone). Like the system acquisition process, the system implementation process must have a high degree of support from the senior executive team and be viewed as an organizational priority. Sufficient staff, time, and resources must be devoted to the project. Individuals involved in rolling out the new system should have the resources available to them to ensure a smooth transition.

The time and resources needed to implement a new health care information system can vary considerably based on the scope of the project, the needs and complexity of the organization, the number of applications being installed, and the number of user groups involved. There are, however, some fundamental activities that should occur during any system implementation regardless of its size or scope.

- Organize the implementation team and identify a system champion
- Determine project scope and expectations
- Establish and institute a project plan

Failing to appropriately plan for and manage these activities can lead to cost overruns, dissatisfied users, project delays, and even system sabotage. In today's environment, where capital is scarce and resources are limited, health care organizations cannot afford to mismanage implementation projects of this magnitude and importance.

Organize the Implementation Team and Identify a System Champion

One of the first steps in planning for the implementation of a new system is to organize an *implementation team*. The primary role and function of the team is to plan, coordinate, budget, and manage all aspects of the new system implementation. Although

the exact team composition will depend on the scope and nature of the new system, a team might include a project leader, system champion(s), key individuals from the clinical and administrative areas that are the focus of the system being acquired, vendor representatives, and IT professionals (Figure 7.1). Having a strong project leader and the right mix of people involved in the implementation planning process is critically important.

Implementation teams often include some of the same people who were involved in selecting the system; however, they may also include other individuals with knowledge and skills important to the successful deployment of the new system. For example, the implementation team will likely need at least one IT professional with technical database and network administration expertise. These persons may have had some role in the selection process but are now being called on to assume a larger role in installing the software, setting up the data tables, and customizing the network infrastructure to adequately support the system and the organization's needs.

The implementation team should also include at least one *system champion*. A system champion is someone who is well respected in the organization, sees the new system as necessary to the organization's achievement of its strategic goals, and is passionate about implementing it. In many health care settings the system champion is a physician, particularly when the organization is implementing a system that will directly or indirectly affect how physicians spend their time. The physician champion serves as an advocate of the system, assumes a leadership role in gaining buy-in from other physicians and user groups, and makes sure that physicians have adequate input into the decision-making process. Other important qualities of physician champions include strong communication skills, interpersonal skills, and good listening skills. The physician champion should be willing to assist with pilot testing, to train and coach others, and to build consensus among user groups (Miller & Sim, 2004). Numerous studies have demonstrated the importance of the system champion throughout the implementation process (Wager, Lee, White, Ward, & Ornstein, 2000; Miller, Sim, & Newman, 2003; Ash, Stavri, Dykstra, & Fournier, 2003).

FIGURE 7.1. SAMPLE COMPOSITION OF IMPLEMENTATION TEAM.



Determine Project Scope and Expectations

One of the implementation team's first items of business is to determine the scope of the project and what the organization hopes the project will achieve. To set the tone for the project, a senior health care executive should meet with the implementation team to communicate how the project relates to the organization's overall strategic goals and to assure the team of administration's commitment to the project.

The goals of the project and what the organization hopes to achieve by implementing the new system should emerge from early team discussions. The system goals defined during the system selection process (discussed in Chapter Six) should be reviewed by the implementation team. Far too often health care organizations skip this important step and never clearly define the scope of the project or what they hope to gain as a result of the new system. At other times they define the scope of the project too broadly.

Let's look at two hypothetical examples, from two providers that we will call Mason Hospital and St. Luke's Medical Center. The implementation team at Mason Hospital defined its goal and the scope of the project and devised measures for evaluating the extent to which the hospital achieved this goal. The implementation team at St. Luke's Medical Center was responsible for completing Phase 1 of a three-part project; however, the scope of the team's work was never clearly defined.

Mason Hospital decided that it wanted to implement a computerized provider order entry (CPOE) system. An implementation team was formed and charged with managing all aspects of the CPOE rollout. Mason Hospital's mission is to be "the premier academic community hospital in the United States." Considering how to achieve this mission, the team identified CPOE as the "building block" needed to improve quality of care, reduce errors, and create a far safer and more effective work environment for hospital medical staff. In addition to establishing this goal, the team went a step further to define what it would consider to be a successful CPOE implementation initiative. Team members developed a core set of metrics (for example, physician CPOE adoption rate, use of telephone and verbal orders in nonemergency situations, reduction in adverse drug events, reduction in duplicate orders, improved quality of documentation, and increased compliance with practice based guidelines) that were subsequently used to track the project's success.

St. Luke's Medical Center set out to implement an EMR system, planning to do so in three phases. Phase 1 involved establishing a clinical data repository, a central database (EMR) from which all ancillary clinical systems would feed, Phase 2 included the implementation of CPOE and nursing documentation systems, and Phase 3 involved the elimination of all outside paper reports through the implementation of a document imaging system. St. Luke's staff felt that if they could complete all three phases they would have, in essence, a "true" EMR. The implementation team did not,

however, clearly define the scope of its work. Was it to complete Phase 1 or all three phases? Likewise, the implementation team never defined what it hoped to accomplish or how implementation of the EMR fit into the medical center's overall mission or organization goals. It never answered the question: How will we know if we are successful? The ambiguity of the implementation team's scope of work led to disillusionment and a sense of failing to ever finish the project.

Establish Project Plan

Once the implementation team has agreed on its goals and objectives, the next major step is to develop and implement a project plan. The project plan should include

- Major activities (also called *tasks*)
- Major milestones
- Estimated duration of each activity
- Any dependencies among activities (for example, one task must be completed before another can begin)
- Resources and budget available
- Individual or members responsible for completing each activity
- Target dates
- Measures for evaluating completion and success

These are the same components one would find in most major projects. What are the major activities, or tasks, that are unique to system implementation projects? Which tasks must be completed first, second, and so forth? How should time estimates be determined and milestones defined?

System implementation projects tend to be quite large, and therefore it can be helpful to break the project into manageable components. One approach to defining components is to have the implementation team brainstorm and identify the major activities that need to be done before the go-live date. Once these tasks have been identified, they can be grouped and sequenced based upon what must be done first, second, and so forth. Those tasks that can occur concurrently should also be identified. A team may find it helpful to use a consultant to guide it through the implementation process. Or the health care IT vendor may have a suggested implementation plan; one must make sure, however, that this plan is tailored to suit the unique needs of the organization in which the new system is to be introduced.

Following are descriptions of the major activities common to most information system implementation projects (listed in Figure 7.2), which may serve as a guide. These activities are not necessarily in sequential order; the order should be determined by the institution based on its needs and resources.

FIGURE 7.2. COMPONENTS OF IMPLEMENTATION PLAN.

1. Workflow and process analysis

- Analyze or evaluate current process and procedures
- Identify opportunities for improvement and, as appropriate, effect those changes
- Identify sources of data, including interfaces to other systems
- Determine location and number of workstations needed
- Redesign physical location as needed

2. System installation

- Determine system configuration
- Order and install hardware
- Prepare computer room
- Upgrade or implement IT infrastructure
- Install software and interfaces
- Customize software
- Test, retest, and test again . . .

3. Staff training

- Train staff
- Update procedure manuals

4. Conversion

- Convert data
- Test system

5. Communications

- Establish communication mechanisms for identifying and addressing problems and concerns
- Communicate regularly with various constituent groups

6. Preparation for go-live date

- Select date when patient volume is relatively low
 - Ensure sufficient staff are on hand
 - Set up mechanism for reporting and correcting problems and issues
 - Review and effect process reengineering
-

Conduct Workflow and Process Analysis. One of the first activities necessary in implementing any new system is to review and evaluate the existing workflow or business processes. Members of the implementation team might also observe the current information system (if there is one) in use. Does it work as described? Where are the problem areas? What are the goals and expectations of the new system? How do organization processes need to change in order to optimize the new system's value and achieve its goals? Too often organizations never critically evaluate current business processes and plunge forward with implementing the new system while still using old procedures. The result is that they simply automate their outdated and inefficient processes.

Before implementing any new system, the organization should evaluate existing procedures and processes and identify ways to improve workflow, simplify tasks, eliminate redundancy, improve quality, and improve user (customer) satisfaction. Although describing them is beyond the scope of this book, many extremely useful tools and methods are available for analyzing workflow and redesigning business processes (see, for example, Davenport & Short, 1990; Hammer & Champy, 1993; Whitten, Bentley, & Dittman, 2004). Simply observing the system in use, listening to the users' concerns, and evaluating information workflow can identify many of the changes needed.

Involving users at this early stage of the implementation process can gain initial buy-in to both the idea and the scope of the process redesign. In all likelihood the organization will need to institute a series of process changes as a result of the new system. Workflow and processes should be evaluated critically and redesigned as needed. For example, the organization may find that as a result of the new system, it needs to do away with forms or work steps, change job descriptions or job responsibilities, or add to or subtract from the work responsibilities of particular departments. Getting users involved in this *reengineering* process can lead to greater user acceptance of the new system.

Let's consider an example. Suppose a multiphysician clinic is implementing a new patient scheduling system. Patients will be able to schedule their own appointments on-line via the Internet, and receptionists will also be able to schedule patient appointments electronically. The clinic might wish to begin by appointing a small team of individuals knowledgeable about analyzing workflow and processes to work with staff in studying the existing process for scheduling patient appointments. This team might conduct a series of individual focus groups with schedulers, physicians and nurses, and patients and ask questions such as

- Who can schedule patient appointments?
- How are patient appointments made, updated, or deleted?
- Who has access to scheduling information? From what locations?
- How well does the current system work? How efficient is the process?
- What are the major problems with the current scheduling system and process? In what ways might it be improved?

The team should tailor the focus questions so they are appropriate for each user group and then reengineer its existing processes and workflow to facilitate the new system.

During the workflow analysis process the team should also examine where the new system's actual workstations will be located, how many workstations will be needed, and how information will flow between users and manual organization processes and the information system. Here are a few of the many questions that should be addressed in ensuring that the physical layout of the area is conducive to the success of the new system.

- Will the workstations be portable or fixed? If users are given portable units, how will these be tracked and maintained (and protected from loss or theft)? Are fixed workstations located in safe, secure areas where patient confidentiality can be maintained?
- How will the user interact with the new system?
- Does the physical layout of the area need to be redesigned to accommodate the new system and the new process?
- Will additional wiring be needed?

Install System Components. The next step, which may be done concurrently with the workflow analysis, is to install the hardware, software, and network infrastructure to support the new information system and build the necessary interfaces. IT staff play a crucial role in this phase of the project. They will need to work with the vendor in determining system specifications and configurations and in preparing the computer room for installation. It may be, for example, that the organization's current computer network will need to be replaced or upgraded.

Typically, when a health care organization acquires a system from a vendor, quite a bit of customization is needed. IT personnel will likely work with the vendor in setting up and loading data tables, building interfaces, and running pilot tests of the hardware and software using actual patient and administrative data. We recommend piloting the system in a unit or area before rolling out the system enterprise-wide. This test enables the implementation team to evaluate the system's effectiveness, address issues and concerns, fix bugs, and then apply the lessons learned to other units in the organization before most people even start using the system.

Consideration should be given to choosing an appropriate area (for example, department or location) or set of users to pilot the system. Some of the questions that the implementation team should consider in identifying potential pilot sites are

- Which units or areas are willing and equipped to serve as a pilot site? Do they have sufficient interest, administrative support, and commitment?
- Are the staff and management teams in each of these units or areas comfortable with being system "guinea pigs"?
- Do staff have the time and resources needed to serve in this capacity?
- Is there a system champion in each unit or area who will lead the effort?

Plan, Conduct, and Evaluate Staff Training. Training is an essential component of any new system implementation. Although no one would argue with this statement, the implementation team will want to consider many issues as it develops and implements a training program. Here are a few of the questions to be answered:

- How much training is needed? Do different user groups have different training needs?
- Who should conduct the training?

- When should the training occur? What intervals of training are ideal?
- At what time and in what place should the training occur?
- What training format is best (for example, formal, classroom-style training; one-on-one or small-group training; a combination of methods)?
- What is the role of the vendor in training?
- Who in the organization will manage or oversee the training? How will training be documented?
- What criteria and methods will be used to monitor training and ensure that staff are adequately trained?

There are various methods of training. One approach, commonly known as *train the trainer*, relies on the vendor to train members of the organization who will then serve as super-users and train others in their respective departments, units, or areas. These super-users should be individuals who work directly in the areas in which the system is to be used; they should know the staff in the area and have a good rapport with them. They will also serve as resources to other users once the vendor representatives have left. They may do a lot of one-on-one training, hand-holding, and other work with people in their areas until these individuals achieve a certain comfort level with the system. The main concern with this approach is that the organization may devote a great deal of time and resources to training the trainers only to have these trainers leave the institution (often because they've been lured away by career opportunities with the vendor).

Another method is to have the vendor train a pool of trainers who are knowledgeable about the entire system and who can rotate through the different areas of the organization working with staff. The trainer pool might include both IT professionals (including clinical analysts) and clinical or administrative staff such as nurses, physicians, lab managers, and business managers.

Regardless of who conducts the training, it is important to introduce fundamental or basic concepts first and allow people to master these concepts before moving on to new ones. Studies among health care organizations that have implemented clinical applications such as CPOE systems have shown that classroom training is not nearly as effective as one-on-one coaching, particularly among physicians (Metzger & Fortin, 2003). Most systems can track physician usage; physicians identified as low-volume users may be targeted for additional training.

Timing of the training is also important. Users should have ample opportunity to practice *before* the system goes live. For instance, when a nursing documentation system is being installed, nurses should have the chance to practice with it at the bedside of a typical patient. Likewise, when a CPOE system is going in, physicians should get to practice ordering a set of tests during their morning rounds. This *just-in-time* training might occur several times: for example, three months, two months, one month, and one week before the go-live date. Additional staff should be on hand during the

go-live period to assist users as needed during the transition to the new system. In general the implementation team should work with the vendor to produce a thoughtful and creative training program.

Once the details of how the new system is to work have been determined, it is important to update procedure manuals and make the updated manuals available to the staff. Designated managers or representatives from the various areas may assume a leadership role in updating procedure manuals for their respective areas. When people must learn specific IT procedures such as how to log in, change passwords, and read common error messages, the IT department should ensure that this information appears in the procedure manuals and that the information is routinely updated and widely disseminated to the users. Procedure manuals serve as reference guides and resources for users and can be particularly useful when training new employees.

Convert Data and Test System. Another important task is to convert the data from the old system to the new system and adequately test the new system. Staff involved in the data conversion must determine the sources of the data required for the new system and construct new files. It is particularly important that data be complete, accurate, and current before being converted to the new system. Data should be *cleaned* before being converted. Once converted, the data should run through a series of validation checkpoints or procedures to ensure the accuracy of the conversion.

IT staff knowledgeable in data conversion procedures should lead the effort and verify the results with key managers from the appropriate clinical and administrative areas. The specific conversion procedures used will depend on the nature of the old system and its structure as well as on the configuration of the new system.

Finally, the new system will need to be tested. The main purpose of the testing is to simulate the live environment as closely as possible and determine how well the system and accompanying procedures work. Are there programming glitches or other problems that need to be fixed? How well are the interfaces working? How does response time compare to what was expected? The system should be populated with live data and tested again. Vendors, IT staff, and user staff should all participate in the testing process. As with training, one can never test too much. A good portion of this work has to be done for the pilot. It may need to be repeated before going live. And the pilot lessons will guide any additional testing or conversion that needs to be done.

Communicate Progress or Status. Equally as important as successfully carrying out the activities discussed so far is having an effective plan for communicating the project's progress. This plan serves two primary purposes. First, it identifies how the members of the implementation team will communicate and coordinate their activities and progress. Second, it defines how progress will be communicated to key constituent groups, including but not limited to the board, the senior administrative

team, departments, and staff at all levels of the organization affected by the new system. The communication plan may set up both formal and informal mechanisms. Formal communication may include everything from regular updates at board meetings and administrative meetings to written briefings and articles in the facility newsletter. The purpose should be to use as many channels and mechanisms as possible to ensure that the people who need to know are fully informed and aware of the implementation plans. Informal communication is less structured but can be equally important.

Prepare for Go-Live Date. A great deal of preparation goes into preparing for the go-live date, the day the organization transitions from the old system to the new. Assuming the implementation team has done all it can to ensure that the system is ready, the staff are well trained, and appropriate procedures are in place, the transition should be a smooth one. Additional staff should be on hand and equipped to assist users as needed. It is best to plan for the system to go live on a day when the patient census is typically low or fewer patients than usual are scheduled to be seen. Disaster recovery plans should also be in place, and staff should be well trained on what to do should the system go down or fail. Designated IT staff should monitor and assess system problems and errors.

A great deal of planning and leadership is needed in implementing a new health care information system. Despite the best-made plans, however, things can and do go wrong. The next section describes some of the common organizational challenges associated with system implementation projects and offers strategies for anticipating and planning for them.

Managing the Organizational Aspects of System Implementation (and Anticipating What Can Go Wrong)

Implementing an information system in a health care facility can have a profound impact on the organization, the people who work there, and the patients they serve. Individuals may have concerns and apprehensions about the new system. They may wonder: How will the new system impact my job responsibilities or productivity? How will my workload change? Will the new system cause me more or less stress? Even individuals who welcome the new system, see the need for it, and see its potential value may worry: What will I do if the system is down? Will the system impede my relationship with my patients? Who will I turn to if I have problems or questions? Will I be expected to type my notes into the system? With the new system comes change, and change can be difficult if not managed effectively.

The human factors associated with implementing a new system should not be taken lightly. A great deal of change can occur as a result of the new system. Some

of the changes may be immediately apparent; others may occur over time as the system is used more fully. Many IT implementation studies have been done in recent years, and they reveal several strategies that may lead to greater organizational acceptance and use of the new system.

- Create an environment where expectations are defined, met, and managed.
- Do not underestimate user resistance.
- Allocate sufficient resources, including technical support staff and IT infrastructure.
- Provide adequate initial and *ongoing* training.

More research is needed to explore further the extent to which these and other factors can lead to more widespread adoption of health care information systems, particularly clinical applications such as the CPOE and EMR systems.

Create an Environment Where Expectations Are Defined, Met, and Managed

If you ask a roomful of health care executives, physicians, nurses, pharmacists, or laboratory managers if they have ever experienced an IT system failure, chances are over half of the hands in the room would go up. In all likelihood the people in the room would have a much easier time describing a system failure than a system success. If you probed a little further and asked why the system was a failure, you might hear comments like these: “the system was too slow,” “it was down all the time,” “training was inadequate and nothing like the real thing,” “there was no one to go to if you had questions or concerns,” “it added to my stress and workload,” and the list goes on. The fact is the system did not meet their expectations. We might not know whether their expectations were reasonable or not.

Earlier we discussed the importance of clearly defining and communicating the goals and objectives of the new system. Related to goal definition is the need to manage user expectations. Different people may have different perspectives on what they expect from the new system; in addition, some will admit to having no expectations, and others will have joined the organization after the system was implemented and consequently are likely to have expectations derived from the people currently using the system.

Expectations come from what people see and hear about the system and the way they interpret what the system will do for them or for their organization. Expectations can be formed from a variety of sources—they may come from a comment made during a vendor presentation, a question that arises during training, a visit to another site that uses the same system, attendance at a professional conference, or a remark made by a colleague in the hallway.

Furthermore, the criterion used to evaluate the system's value or success depends on the individual's expectations and point of view. For example, the CFO might measure success in terms of the system's financial return on investment, the chief medical director might look at its impact on physicians' time and quality of care, the nursing staff might assess its value based on their workload, public relations personnel might assess the system's impact on patient satisfaction, and the IT staff might evaluate the change in the number of help desk calls made since the new system was implemented. All of these approaches are measures of an information system's perceived impact on the organization or individual. However, they are not all the same, and they may not have equal importance to the organization in achieving its strategic goals.

It is therefore important for the health care executive team not only to establish and communicate clearly defined goals for the new system but also to listen to needs and expectations of the various user groups and manage expectations appropriately. Ways to manage expectations include making sure users understand that the first days or weeks of systems use may be rocky, that the organization may need time to adjust to a new workflow, that the technology may have bugs, and that users should not expect problem-free system operation from the start. Clear and effective communication is key in this endeavor.

Do Not Underestimate User Resistance

During the implementation process it is important to analyze current workflow and make appropriate changes as needed. Earlier we gave an example of analyzing a patient scheduling process. Patient scheduling is a relatively straightforward process. A change in this system may not dramatically change the job responsibilities of the schedulers and may have little impact on nurses' or physicians' time. Therefore these groups may offer little resistance to such a change. (This is not to guarantee a lack of resistance—if you mess up a practice's schedule, you can have a lot of angry people on your hands!) In contrast, processes that involve the direct provision of patient care services and that do affect nurses' and physicians' time may be tougher for users to accept. The physician ordering process is a perfect example. Most physicians today are accustomed to picking up a pen and paper and handwriting an order or calling one in to the nurses' station from their phones. With computerized provider order entry (CPOE), physicians may be expected to keyboard their orders directly into the system and respond to automated reminders and decision-support alerts. A process that historically took them a few seconds to do might now take several minutes, depending on the number of prompts and reminders. Moreover, physicians are now doing things that were not asked of them before—they are checking for drug interactions, responding to reminders and alerts, evaluating whether evidence-based clinical guidelines apply to the patient, again the list goes on. All these activities take time, but in the long run they will improve the

quality of patient care. Therefore it is important for physicians to be actively involved in designing the process and in seeing its value to the patient care process.

Getting physicians, nurses, and other clinicians to accept and use clinical information systems such as CPOE or EMR can be challenging even when they are involved in the implementation. At times the incentives for using the system may not be aligned with their individual needs and goals. On the one hand, for example, if the physician is expected to see a certain number of patients per day and is evaluated on patient load and if writing orders used to take thirty minutes a day with the old system and now takes sixty to ninety minutes with the new CPOE system, the physician can either see fewer patients or work more hours. One should expect to see physician resistance. On the other hand, if the physician's performance and income is related to adherence to clinical practice guidelines, using the CPOE system might improve his or her income, creating a greater chance of acceptance.

The physician's workload or productivity goals might, however, be beyond the organization's control. They might be individual goals the physician has set for himself or herself. Can or should organizations mandate the use of clinical information systems like CPOE? In effect, the organization is stating that resistance is unacceptable. Several health care facilities have instituted policies mandating physician use of CPOE, with mixed results. Physicians' acceptance of such a mandate may have a lot to do with the organization culture, the training they received, their confidence (or lack of confidence) in the system, how the mandate was imposed, and a host of other factors. Mandating use is most common in academic medical centers where residents and fellows are expected to enter orders. Mandating physician use can be taxing in community hospitals or facilities where physicians are not employed. Community-based physicians often admit patients to more than one hospital and spend limited time at each facility. Trying to get the fairly independent physician to buy into the CPOE system and participate in the necessary training can be difficult.

To address this and related acceptance issues, the California HealthCare Foundation, in collaboration with First Consulting Group, conducted an in-depth study of ten community hospitals through the United States that have made significant progress in implementing CPOE (Metzger & Fortin, 2003). The study found that CPOE leaders tended to avoid the term *mandate* and instead recommended that health care executives work toward an enterprise-wide policy for universal CPOE. Key staff in participating hospitals recommended starting with a strong commitment to CPOE, delivering a consistent message that CPOE is the right thing to do and working within the culture of the medical staff toward the goal of universal adoption. This goal might take years to achieve. Readiness for universal adoption occurred once (1) a significant number of physician CPOE adopters showed their peers what was possible, (2) sufficient progress was made toward achieving patient safety objectives, and (3) the medical staff came together with one voice to champion CPOE as the right thing to do.

Mandating use or adopting a universal acceptance policy may be needed but should come with time. Experience has shown that a mandate should not be imposed until the organization has achieved a certain level of use, there is confidence in the system's functionality, and adequate buy-in from the medical staff exists. There may be a point in time where all orders will be entered directly by physicians or when paper medical records will no longer be pulled or maintained. However, that point in time should be clearly communicated, all efforts should be made to ensure users are trained and ready to make the change, and backup procedures should be in place when the day arrives.

System champions, particularly physician champions, can be extremely helpful in preparing for the day of universal adoption. They can serve as coaches, listeners, teachers, and advocates for facility physicians and for the system. It is through their role and example that others will come along. Some may choose not to and may leave the organization; however, the great majority will stay and work toward the common goal.

It perhaps goes without saying that user acceptance occurs when users see or realize the *value* the health care information system brings to their work and the patients they serve. This value takes different forms. Some people may realize increased efficiency, less stress, greater organization, and improved quality of information, whereas others may find that the system enables them to provide better care, avoid medical mistakes, and make better decisions. In some cases an individual may not experience the value personally but may come to realize the value to the organization as a whole.

Allocate Sufficient Resources, Including Technical Support Staff and IT Infrastructure

Sufficient resources are needed both during and after the new system has been implemented. User acceptance comes from confidence in the new system. Individuals want to know that the system works properly, is stable, and is secure and that someone is available to help them when they have questions, problems, or concerns. Therefore it is important for the organization to ensure that adequate resources are devoted to implementing and supporting the system and its users. At a minimum, adequate technical staff expertise should be available as well as sufficient IT infrastructure.

We have discussed the importance of giving the implementation team sufficient support as it carries out its charge, but what forms can this support take? Some methods of supporting the team are to make available release time, additional staff, development funds, and travel funds to enable staff to view the system in use in other facilities. Senior management might decide that all implementation team members or super-users will receive 50 percent release time for the next six months to devote to the project. This release time will enable those involved to give up some of their normal job duties so they can focus on the project. Senior leaders at one health care organization in South Carolina gave sixty-four full-time staff release time for one year to devote to the

implementation of a facility-wide hospital information system. This substantial amount of release time was indicative of the high value the executive team members placed on the project. They saw it as critical to achieving the organization's strategic goals.

Providing sufficient time and resources to the implementation phase of the project is, however, only part of the overall support needed. Studies have shown that an information system's value to the organization is typically realized over time. Value is derived as more and more people use the system, offer suggestions for enhancing it, and begin to push the system to fulfill its functionality. If users are ever to fully realize the system's value, they must have access to local technical support—someone, preferably within the organization, who is readily available, is knowledgeable about the intricacies of the system, and is able to handle both hardware and software problems. This individual should be able to work effectively with the vendor and others to find solutions to system problems. Even though it is ideal to have local technical support in-house, that may be difficult in small physician office or community-based settings. In such cases the facility may need to consider such options as (1) devoting a significant portion of an employee's time to training so that he or she may assume a support role, (2) partnering with a neighboring organization that uses the same system to share technical support staff, or (3) contracting with a local computer firm to provide the needed assistance. The vendor may be able to assist in identifying resources locally to assist the organization in securing local technical support.

In addition to arranging for local technical support, the organization will also need to invest resources in building and maintaining a reliable, secure IT infrastructure (servers, operating systems, and networks) to support the information system, particularly if it is a mission-critical system. Many patient information systems need to be available 24 hours a day, 7 days a week, 365 days a year. Health care professionals can come to rely on having access to timely, accurate, and complete information in caring for their patients, just as they count on having electricity, water, and other basic utilities. Failing to build the IT infrastructure that will adequately support the new clinical system can be catastrophic for the organization and its IT department.

An IT infrastructure's lifetime may be relatively short. It is reasonable to expect that within three to ten years, the hardware, software, and network will likely need to be replaced as advances are made in technology, the organization's goals and needs change, and the health care environment changes.

Provide Adequate Initial and Ongoing Training

Earlier we discussed the importance of training staff on the new system prior to the go-live date. Having a training program suited to the needs of the various user groups

is very important during the implementation process. People who will use the system should be relatively comfortable with it, have had ample opportunities to use it in a safe environment, and know where to turn should they have questions or need additional assistance. It is equally important to provide *ongoing* training months and even years after the system has been implemented. In all likelihood the system will go through a series of upgrades, changes will be made, and users will get more comfortable with the fundamental features and will be ready to push the system to the next level. Some users will explore additional functionality on their own; others will need prodding and additional training in order to learn more advanced features.

When implementing a new system, it is important to view the system as a long-term investment rather than a one-time purchase. The resources allocated or committed to the system should include not only the upfront investment in hardware and software but also the time, people, and resources needed to maintain and support it.

System Maintenance and Support

Information systems evolve as an organization continues to grow and change. No matter how well the system was designed and tested, errors and problems will be detected and changes will need to be made. IT staff generally assume a major role in maintaining and supporting the information systems in the health care organization. When errors or problems are detected, IT staff correct the problem or work with the vendor to see that the problem is fixed. Moreover, the vendor may detect glitches and develop upgrades or patches that will need to be installed.

Many opportunities for enhancing and improving the system's performance and functionality will occur well after the go-live date. The organization will want to ensure that the system is adequately maintained, supported, and further developed over time. Selecting and implementing a health care information system is an enormous investment. This investment must be maintained, just as one would maintain one's home.

Like any other device, information systems have a *lifecycle* and eventually need to be replaced. Likewise, health care organizations typically go through a process whereby they plan, design, implement, and evaluate their health care information systems. Too often in the past the organization's work was viewed as done once the system went live. It has since been discovered how vital system maintenance and support resources are and how important it is to evaluate the extent to which the system goals are being achieved.

Summary

Implementing a new information system in a health care organization requires a significant amount of planning and preparation. The health care organization should begin by appointing an implementation team comprising experienced individuals, including representatives from key areas in the organization, particularly areas that will be affected by or responsible for using the new system. Key users should be involved in analyzing existing processes and procedures and making recommendations for changes. A system champion should be part of the implementation team and serve as an advocate in soliciting input, representing user views, and spearheading the project. When implementing a clinical application, it is important that the system champion be a physician or clinician, someone who is able to represent the views of the care providers.

Under the direction of a highly competent implementation team, a number of important activities should occur during the system rollout. The implementation team should assume a leadership role in ensuring that the system is effectively incorporated into the day-to-day operations of the facility. This generally requires the organization to (1) analyze workflow and processes and perform any necessary process reengineering, (2) install and configure the system, (3) train staff, (4) convert data, (5) adequately test the system, and (6) communicate project progress using appropriate forums at all levels throughout the organization. Attention should be given to the countless details associated with ensuring that backup procedures are in place, security plans have been developed, and the organization is ready for the go-live date.

During the days immediately following system implementation, the organization should have sufficient staff on hand to assist users and provide individual assistance as needed. A stable and secure IT infrastructure should be in place to ensure minimal, ideally zero, downtime and adequate response time. The IT department or other appropriate unit or representative should have a formal mechanism in place for reporting and correcting errors, bugs, and glitches in the system.

Once the system has gone live, it is critical for the organization to have in place the plans and resources needed to adequately maintain and support the new system. Technical staff and resources should be available to the users. Ongoing training should be an integral part of the organization's plans to support and further develop the new system.

Beyond taking ultimate responsibility for completion of the activities needed to implement and support the new system, the health care executive should assume a leadership role in managing the organizational and human aspects of the new system. Information systems can have a profound impact on health care organizations, the people who work there, and the patients they serve. Acquiring a good product and

having the right technical equipment and expertise is not enough to ensure system success. Health care executives must also be attuned to the human aspects of introducing new IT into the care delivery process.

Chapter Seven: Learning Activities

1. Visit a health care organization that has recently implemented a health care information system. What process did it use to implement the system? How does that process compare with the one described in this chapter? How successful was the organization in implementing the new system? To what do staff attribute this success?
2. Search the literature for a recent article on a system implementation project. Briefly describe the process used to implement the system and the lessons learned. How might this particular facility's experiences be useful to others? Explain.
3. Physician acceptance and use of clinical information systems is often cited as a challenge. What do you think the health care leadership team can or should do to foster acceptance by physicians? Assume a handful of physicians in your organization are actively resisting a new clinical information system. How would you approach and address their resistance and concerns?
4. Assume you are working with an implementation team in installing a new nursing documentation system for a home health agency. Historically, all its nursing documentation was recorded in paper form. The home health agency has little computerization beyond basic registration information and no IT staff. What recommendations might you offer to the implementation team as it begins the work of installing the new nursing documentation system?
5. Discuss the risks to a health care organization in failing to allocate sufficient support and resources to a newly implemented health care information system.
6. Assume you are the CEO of a large group practice (seventy-five physicians) that implemented an EMR system two years ago. The physicians are asking for an evaluation of the system and its impact on quality, costs, and patient satisfaction. Devise a plan for evaluating the EMR system's impact on the organization in these three areas.



PART THREE

INFORMATION TECHNOLOGY



CHAPTER EIGHT

INFORMATION ARCHITECTURE AND TECHNOLOGIES THAT SUPPORT HEALTH CARE INFORMATION SYSTEMS

Thus far in this text we have explored a variety of health care information systems. These systems have been presented with minimal discussion of the technology behind them. The focus has instead been on how the various applications are adopted, implemented, and used. Although we do not believe that health care executives need to become information technology (IT) experts in order to make informed decisions about which health care information systems to employ in their organizations, we do believe that an exposure to some of the core technologies used to develop and implement common health care information systems is quite useful. This knowledge will help health care executives be more informed decision makers.

This chapter provides a broad view of several categories of core, or base, technologies. They are not unique to health care but are frequently found in health care organizations. We discuss technologies used in each of the following categories:

- System software
- Data management and access
- Networks and data communications
- Information processing distribution schemes
- The Internet, intranets, and extranets
- Clinical and managerial decision support
- Trends in user interactions with systems

We will end with a discussion of the concept of system architecture, or how all the technologies “fit together” within an organization to support health care applications. Like many fields, IT has its own language. It is helpful for health care executives to learn IT terminology and concepts so they can communicate effectively with IT staff and vendors.

System Software

Up to this point we have discussed health care information system applications without looking at the technologies on which they run. In this section we will begin with a general discussion of software and then define programming languages, operating systems, and interface engines.

There are two basic types of software, *systems software* and *applications software*. These two types of software have a common characteristic: both represent a series of computer programs. Remember that at its most basic level of functioning the computer recognizes two things, an electrical impulse that is on and an electrical impulse that is off; these signals are often represented as 0 and 1 (or *bits*). A human programmer must write programming code to translate the desires of the user into computer actions. There are many different programming languages in use today, and they are continue to evolve.

Machine languages are the oldest computer programming languages. Machine language programmers had to literally translate each character or operator into binary code, displayed as groups of 0s and 1s. Machine languages are often referred to as *first generation languages*. Fortunately, by the 1950s, *assembly languages*, the *second generation languages*, were developed, which simplified machine language programming. The *procedural programming languages* (*third generation*), for example, FORTRAN and COBOL, came along shortly after the assembly languages, allowing programmers to write computer programs without being as concerned with manually producing the machine language. Today, *fourth generation languages* (4GLs), which have many preprogrammed functions, allow individuals to develop applications without writing a single line of program code themselves. The software creates the code in the background, invisibly from the developer’s point of view. In the data management section we will discuss *structured query language* (SQL), which is an example of a 4GL.

Two other types of programming frequently used today are *visual programming* and *object-oriented programming*. The most common type of visual programming is Microsoft’s Visual Basic, which allows developers to see the final visual appearance of an application, such as the buttons, scroll-down menus, and windows, as they develop the application. The object-oriented languages differ from traditional procedural languages in that they allow the programmer to create *objects* that include the operations (methods) linked to the data. For example, a master patient index (MPI) object would contain

both the MPI data, such as medical record number, last name, first name, and so forth, and the procedures that use this data, such as assigning the medical record number, retrieving patient names by medical record number, and so forth. Object-oriented languages allow *chunks* of code to be reused and facilitate program maintenance. Common object-oriented programming languages are C++ and Java. A full discussion of programming languages is beyond the scope of this book, but as health care executives you may hear the IT professionals talk about different types of programming languages such as C++, Visual Basic, or Java.

Operating Systems

System software is a series of programs that carry out basic computing functions: for example, managing the user interface, files, and memory. System software also operates any peripherals linked to the computer, such as printers, monitors, and other devices. System software is what allows developers to create applications without having to include basic computer instructions. The most important component of system software is the *operating system*. The operating system is loaded when a computer is turned on and it is responsible for managing all other programs that are subsequently used by the computer. Common types of operating systems are Windows (in several different versions), Mac OS, Unix, and Linux.

Operating systems may be *proprietary* or *open source*. Proprietary operating systems, such as Windows and Mac OS, are purchased, and the actual source code (programs) is not made available to purchasers. The most popular operating systems are proprietary. However, in the 1990s open source (or nonproprietary) operating systems became viable when a Finnish graduate student, Linus Torvald, developed a variant of the operating system Unix, called Linux. Torvald never claimed rights to that operating system, and it is widely available via the Internet. As Linux gains popularity, software companies, such as Intel, Informix, and Netscape have begun to support it (Oz, 2004).

Interface Engines

An *interface engine* is “a software program designed to simplify the creation and management of interfaces between application systems” (Altis, 2004). Interfaces between applications became increasingly important as health care systems moved from *best of breed* to more integrated architectures. (These architecture distinctions will be discussed at the end of the chapter.) Users wanted their various applications to be able to *talk* to one another. They wanted to eliminate the need for entering patient demographic information multiple times into separate systems, for example. In fact, users began to ask for a *single sign-on system* so they could access all the information they needed through a single user interface.

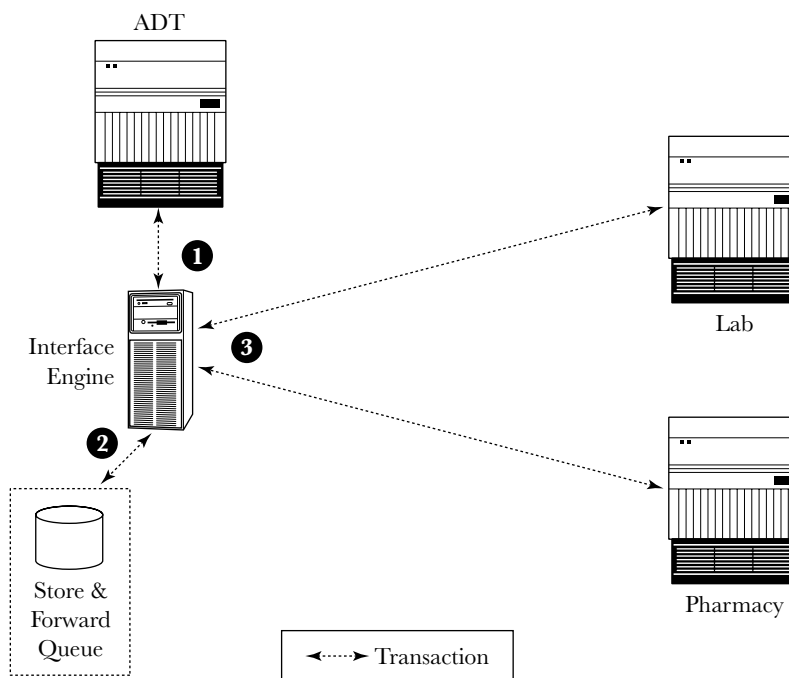
Interface engines are actually a form of *middleware*, a class of software that works “between” or “in the middle” of applications and operating systems. Other examples of middleware are applications that check for viruses, medical logic processors, and data encryption software. A typical interface engine operates in three basic steps. Figure 8.1 illustrates a typical one-to-many transaction involving a hospital admission/discharge/transfer (ADT) system. Here, the ADT system needs to communicate to the lab and pharmacy systems that a patient has been admitted. The ADT system sends a message with the relevant demographic and account detail to the interface engine. The interface engine receives the message, processes it as necessary, and places it in a *queue*, or wait line, for delivery to the lab and pharmacy systems. The message is subsequently forwarded from the queue to those systems. Some interface engines can handle many-to-many transactions as well as one-to-many transactions. Messages are received by the interface engine from multiple systems and are then forwarded to multiple systems.

Data Management and Access

All the health care applications discussed thus far require data. The EMR relies on comprehensive databases, as do other clinical applications. Data must be stored and maintained so that they can be retrieved and used within the applications. In this section we discuss common types of databases and the database management systems with which they are associated. The majority of our discussion centers on the *relational database* because it is the type of database most commonly developed today. Two older types of databases, hierarchical and network (not be to confused with a computer network), may still exist in health care organizations as components of older, legacy applications, but because they no longer have a significant presence in the database market, they are not discussed here. A fourth type of database, the *object-oriented database*, has received a lot of attention in the literature during the past few years. Although a “pure” object-oriented database is not yet common in the health care market, there are applications with object-oriented components built upon relational databases. This hybrid database type is referred to as an *object-relational database*.

Relational Databases

Relational databases were first developed in the early 1970s (Rob & Coronel, 2004). These early relational databases were not practical, however, because they required so much processing power. As computers became more powerful in the 1980s and 1990s, the role of relational databases became more significant. Today the relational database

FIGURE 8.1. COMMON INTERFACE ENGINE OPERATION.

Source: Copyright © by Altis Inc. Reprinted with permission.

is the predominant type used in health care and business. A relational database is implemented through a *relational database management system* (RDBMS). Microsoft Access is an example of an RDBMS for desktop computing; Oracle, Sybase, and Microsoft SQL Server are examples of the more robust RDBMS that are used to develop larger applications.

An application developed using a RDBMS has three distinct components, or layers (Figure 8.2). The interface is developed using software such as Visual Basic or Java. In Microsoft Access this layer is created with Visual Basic for Applications (VBA), which is built into the Access package and used to create the forms and reports that make up the majority of the user interface. The bottom layer of the RDBMS is created with a special type of software, a *data definition language* (DDL). The DDL creates the database table structure and the relationships among the various tables. Each table can be thought of as a file, with each row in the table being a record and each column being

FIGURE 8.2. RELATIONAL DATABASE MANAGEMENT SYSTEM COMPONENTS.

Interface Variety of computer languages (VBA, Java, Delphi, and so forth)
Data Manipulation Data Manipulation Language (DML)
Tables Data Definition Language (DDL)

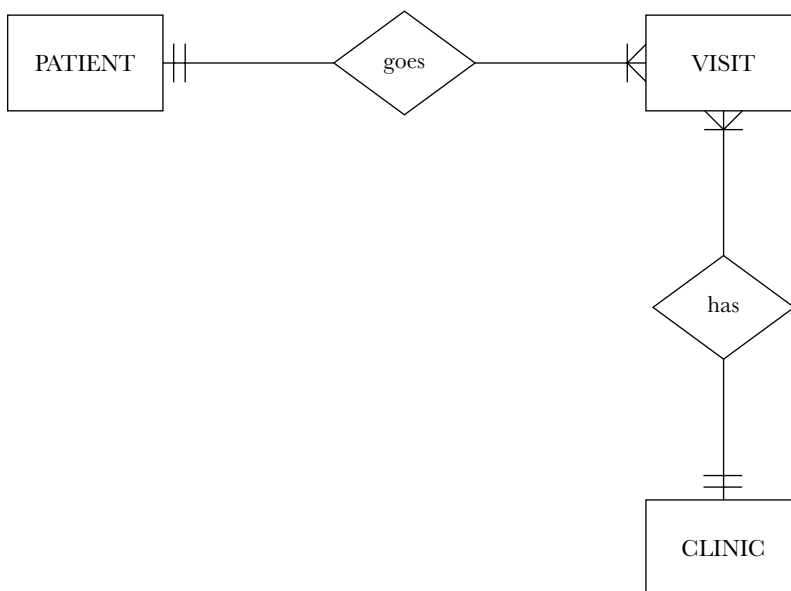
a field or piece of data. In between the data tables and the interface a RDBMS has a *data manipulation layer*. The functions of this layer are performed by a *data manipulation language* (DML). The DML is the software that allows the user to retrieve, query, update, and edit the data in the underlying tables.

The language most widely used for both the DLL and DML functions in relational databases is *structured query language* (SQL). SQL is an example of a 4GL. The user or programmer specifies what must be done but not “how” it must be done. In other words the programmer does not need to design the complex actions the computer takes when an SQL command is executed. SQL is recognized as a de facto standard for relational database functioning. The common RDBMS products support some type of SQL, but many of them also employ extensions to the basic language.

To further support interoperability among databases using different management systems, the *Open Database Connectivity* (ODBC) standard was developed for database *application program interface* (API). This standard is closely aligned with SQL, was developed by the SQL Access Group, and was first released in 1992. ODBC allows programs to use SQL requests without having to know the proprietary interfaces to the databases (Whatis?com, 2002). Using databases that comply with the ODBC standard allows a health care organization to more easily integrate its databases. The organization can move data from ODBC-compliant PC-based application programs on databases to larger databases and vice versa, for example.

Perspective: Relational Data Modeling

Figure 8.3 is an example of an entity relationship diagram (ERD), which graphically depicts the tables and relationships in a simple relational database. Data modeling is

FIGURE 8.3. ENTITY RELATIONSHIP DIAGRAM.

an important tool for database designers. These models are frequently used not only as “blueprints” for building databases but also as tools for communication between the designers and the eventual users. Although a complete discussion of ERDs (and data modeling in general) is beyond the scope of this book, we will point out several key components of the model here. ERDs are often used as communication tools by database developers. Therefore it may be necessary for the health care executive to have a cursory understanding of their components.

Entities. The rectangles in the ERD represent entities. An *entity* is a person, place, or thing about which the organization wishes to store data. The entities depicted in the final version of the ERD will be transformed into tables in the relational database. Figure 8.4 shows an example of a table structure that might be created from the entity CLINIC. (Please note that these examples are quite simplistic and meant to illustrate general concepts rather than represent actual database design practices.)

Attributes. The attributes of an ERD can be shown as oval shapes extending from the entities; however, it is more common to see the entities listed separately or within

**FIGURE 8.4. PARTIAL ATTRIBUTE LISTS FOR *PATIENT*,
CLINIC, AND *VISIT*.**

PATIENT ENTITY ATTRIBUTES

PATIENT_MRN (PK)
PATIENT_LNAME
PATIENT_FNAME
PATIENT_MNAME
PATIENT_SSN
PATIENT_STREET
PATIENT_CITY
PATIENT_STATE
PATIENT_ZIPCODE
PATIENT_PHONE
PATIENT_DOB
...

VISIT ENTITY ATTRIBUTES

VISIT_ID (PK)
VISIT_DATE
VISIT_REASON
PATIENT_MRN (FK)
CLINIC_ID(FK)
...

CLINIC ENTITY ATTRIBUTES

CLINIC_ID (PK)
CLINIC_NAME
CLINIC_STREET
CLINIC_CITY
CLINIC_STATE
CLINIC_ZIPCODE
CLINIC_PHONE
CLINIC_FAX
...

the entity rectangle (see Figure 8.4). Attributes transform to data fields. Each entity in the ERD must have a unique identifier, called its *primary key*. The primary key cannot be duplicated within a table and cannot contain a null value. The primary key is also used to link entities together in order to form relationships.

Relationships. Relationships within ERDs may be shown as diamond shapes. The name of the relationship is usually a verb. There are three possible relationships among any two entities: one-to-one, one-to-many, or many-to-many. Many-to-many relationships must be converted to one-to-many before a relational database can be

implemented. In our ERD example (Figure 8.3), the *one* side of a relationship is shown by a single mark across the line and the *many* side is shown with a three-pronged crow's foot. To decipher the relationship between PATIENT and VISIT as shown in Figure 8.3, you would say, "for each instance of PATIENT there are many possible instances of VISIT, and for each instance of VISIT there is only one possible instance of PATIENT."

Preparing a data model to include only those relationships that can and should be implemented in the resulting database is called *normalization*. Normalizing the database ensures that data are stored in only one location in the database (except for planned redundancy). Storing each piece of data in only one location decreases the possibility of data anomalies as a result of additions and deletions. This reduction in data redundancy and decreased potential for data anomalies is the hallmark of a relational database. It is what distinguishes it from the flat file, an older database model.

Object-Oriented Databases

A newer database structure is the *object-oriented database* (OODB). The basic component in the OODB is an object rather than a table. An object includes both data and the relationships among the data in a single conceptual structure. An *object-oriented database management system* (OODBMS) uses *classes* and *subclasses* that inherit characteristics from one another in a hierarchical manner. Think, for example, of mammals as one class of animals in the physical world (with reptiles being another class) and humans as one subclass of mammals. Because all mammals have hair, humans "inherit" this characteristic. Object subclasses "inherit" properties from an object class in a similar manner. If a "person" object is defined as having a last name and a first name variable, then any subclass objects, such as "patient," will "inherit" these definitions. The "patient" object may also have additional characteristics. A pure OODB is not common in the health care market, but products are beginning to incorporate elements of OODB and object-oriented programming with relational databases (Lee, 2002).

The *object-relational database management system* (ORDBMS) is a product that has relational database capabilities plus the ability to add and use objects. One example on the market today is ObjectStore. The advantage of an ORDBMS is that many of the newer health care applications use video and graphical data, which an ORDBMS can handle better than a traditional RDBMS can. An ORDBMS also has the capability of incorporating hypermedia and spatial data technology. Hypermedia technology allows data to be connected in *web* formations, with hyperlinks. Spatial data technology allows data to be stored and accessed according to locations (Stair & Reynolds, 2003).

Data Dictionaries

One very important step in developing a database to use in a health care application is the development of the *data dictionary*. The data dictionary gives both users and developers a clear understanding of the data elements contained in the database. Confusion about data definitions can lead to poor-quality data and even to poor decisions based on data misconceptions. A typical data dictionary allows for the documentation of

- Table names
- All attribute or field names
- A description or definition of each data element
- The data type of the field (text, number, date, and so forth)
- The format of each data element (such as DD-MM-YYYY for the date)
- The size of each field (such as 11 characters for a Social Security Number, including the dashes)
- An appropriate range of values for the field (such as integers 000000—999999 for a medical record number)
- Whether or not the field is required (is it a primary key or linking key?)
- Relationships among fields

The importance of a well thought out data dictionary cannot be overstated. When one is trying to link or combine databases, the data dictionary is a vital tool. Think, for example, how difficult it might be to combine information from databases with different definitions for fields with the same name.

Clinical Data Repositories

Many health care organizations, particularly those moving toward electronic medical records, develop *clinical data repositories*. Although these databases can take different forms, in general, the clinical data repository is a large database that gets data from various data stores within application systems across the organization. There is generally a process by which data are *cleaned* before they are moved from the source systems into the repository. Once the clean data are in the repository, they can be used to produce reports that integrate data from two or more data stores.

Data Warehouses and Data Marts

A *data warehouse* is a type of large database designed to support decision making in an organization. Traditionally, health care organizations have collected data in a variety of *on-line transactional processing* (OLTP) systems, such as the traditional relational database

and clinical data repository. OLTP systems are well suited for supporting the daily operations of a health care organization but less well suited for decision support. Data stored in a typical OLTP system are always changing, making it difficult to track trends over time, for example. The data warehouse, in contrast, is specifically designed for decision support. It differs from the traditional OLTP database in several key areas, summarized in Table 8.1.

Like a clinical data repository, a data warehouse stores data from other database sources. Creating a data warehouse involves extracting and cleaning data from a variety of organizational databases. However, the underlying structure of a data warehouse is different from the table structure of a relational database. This different structure allows data to be extracted along such dimensions as time (by week, month, or year), location, or diagnosis. Data in a data warehouse can often be accessed via *drill-down*

TABLE 8.1. DIFFERENCES BETWEEN OLTP DATABASES AND DATA WAREHOUSES.

Characteristic	OLTP Database	Data Warehouse
Purpose	Support transaction processing	Support decision support
Source of data	Business transactions	Multiple files, databases—data internal and external to the firm
Data access allowed to users	Read and write	Read only
Primary data access mode	Simple database update and query	Simple and complex database queries with increasing use of data mining to recognize patterns in the data
Primary database model employed	Relational	Relational
Level of detail	Detailed transactions	Often summarized data
Availability of historical data	Very limited—typically a few weeks or months	Multiple years
Update process	On-line, ongoing process as transactions are captured	Periodic process, once per week or once per month
Ease of update	Routine and easy	Complex, must combine data from many sources; data must go through a data cleanup process
Data integrity issues	Each individual transaction must be closely edited	Major effort to clean and integrate data from multiple sources

Source: *Principles of Information Systems, 6th Edition*, by STAIR/REYNOLDS. © 2004. Reprinted with permission of Course Technology, a division of Thomson Learning: www.thomsonrights.com. Fax 800-730-2215.

menus that allow you to see smaller and smaller units within the same dimension. For example, you could view the number of patients with a particular diagnosis for a year, then a month in that year, then a day in that month. Or you could see how many times a procedure was performed at all locations in the health system, then see the total by region, then by facility. Even though the same data might be available in a relational database, its normalized structure makes the queries you would have to use to get at the information quite complex and difficult to execute. Data warehouses help organizations transform large quantities of data from separate transactional files into a single decision support database. *Data marts* are structurally similar to data warehouses but generally not as large. The typical data mart is developed for a particular purpose or unit within an organization.

Data Mining

Data mining is another concept closely associated with large databases such as clinical data repositories and data warehouses. However, data mining (like several other IT concepts) means different things to different people. Health care application vendors may use the term *data mining* when referring to the user interface of the data warehouse or data repository. They may refer to the ability to drill down into data as *data mining* for example. However, more precisely used, *data mining* refers to a sophisticated analysis tool that automatically discovers patterns among data in a data store. Data mining is an advanced form of decision support. Unlike passive query tools, the data mining analysis tool does not require the user to pose individual specific questions to the database. Instead, this tool is programmed to look for and extract patterns, trends, and rules. True data mining is currently used in the business community for marketing and predictive analysis (Stair & Reynolds, 2003). This analytical data mining is, however, not currently widespread in the health care community.

Networks and Data Communications

The term *data communications* refers to the transmission of electronic data within or among computers and other related devices. In this section we will take a cursory look at many of the components that go into building computer networks for the purpose of data communications. (Although the Internet is certainly a part of the overall data communications system that health care organizations use, we believe it is significant enough to warrant its own section, which follows this one.)

Devices that make up computer networks must be compatible. They must be able to communicate with one another. Much of what we introduce in this chapter takes the form of definitions and examples of different types of network components whose compatibility and interoperability might be an issue. Specifically, we will cover the

following topics as they relate to data communications, particularly in health care settings:

- Network communication protocols
- Network types and configurations
- Network media and bandwidth
- Network communication devices

Network Communication Protocols

Data communication across computer networks is possible today because of *communication protocols and standards*. Without the common *language* of protocols, networked computers and other devices would not be able to connect with and talk to one another.

The distinction between protocols and standards is often misunderstood. On the one hand the English language is a protocol for communication. It is also a standard. People taught English by different instructors in different parts of the globe will learn (more or less) the same thing and be able to communicate with each other because there is a standard vocabulary and standards for such things as verb tense. On the other hand the plugs for appliances are protocols—there is a specification for the two flat prongs that form the plug. But the plug is not a standard. Appliances in Switzerland use two round prongs and an American appliance cannot be plugged into a Swiss outlet.

The need for standard network protocols has been evident since the first computer networks were built. To this end the International Organization for Standardization developed the *Open Standards Interconnection (OSI)* model. Work on OSI was begun in the 1980s. Although this model has been well accepted as a *conceptual*, or *reference*, model for network protocols, it is important to be aware that it has not evolved into detailed specifications, as was once anticipated (WhatIs?com, 2002). OSI is not a set of protocols. Rather, it is a model, or scheme, for describing network protocols that have been or will be developed and adopted by the industry. A general introduction to OSI is useful as a point of reference when discussing other aspects of computer networks. Table 8.2 provides a brief description of each of the layers of the OSI model. Figure 8.5 depicts the conceptual framework, showing how data would flow from one computer to another on the network.

To date, the network model most commonly adopted for creating software for network communications has been the *Internet model*, which employs *Transmission Control Protocol/Internet Protocol (TCP/IP)*. TCP/IP was first introduced in the 1970s by the U.S. government to support defense activities (Stair & Reynolds, 2003). However, it was not until the boom of the World Wide Web that this set of protocols began to dominate the computer network industry. Like the OSI model, the Internet model is a layered model (Figure 8.6). However, the Internet model has fewer layers, and unlike the OSI reference model, it represents actual protocol specifications at each layer (White, 2001).

TABLE 8.2. SEVEN-LAYER OSI MODEL.

Application (Layer 7)	This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application specific. This layer provides application services for file transfers, e-mail, and other network software services.
Presentation (Layer 6)	This layer provides independence from differences in data representation (for example, encryption) by translating from application to network format and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems.
Session (Layer 5)	This layer establishes, manages, and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.
Transport (Layer 4)	This layer provides transparent transfer of data between end systems, or hosts. It ensures complete data transfer.
Network (Layer 3)	This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, Internet working, error handling, congestion control, and packet sequencing.
Data Link (Layer 2)	At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control, and frame synchronization. The data link layer is divided into two sublayers: the media access control (MAC) layer and the logical link control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control, and error checking.
Physical (Layer 1)	This layer conveys the bit stream—electrical impulse, light, or radio signal—through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards, and physical aspects. Fast Ethernet and ATM are protocols with physical layer components.

Source: Based on webopedia.com, 2004b.

FIGURE 8.5. DATA FLOW IN THE OSI MODEL.

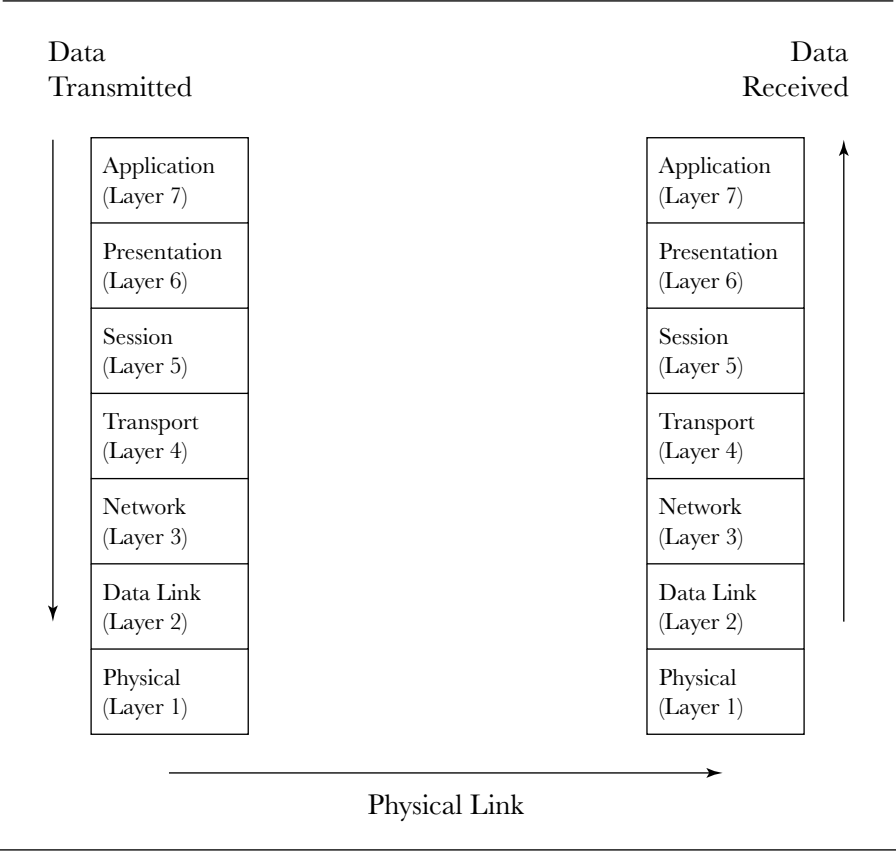
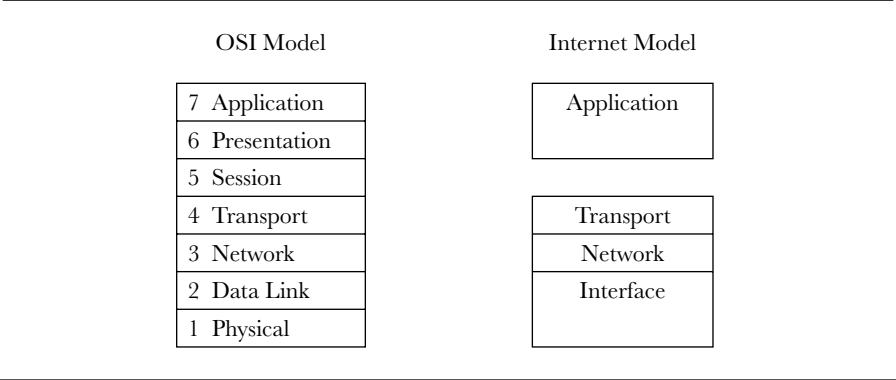


FIGURE 8.6. OSI MODEL COMPARED TO THE INTERNET MODEL.



A few other standard network protocols are also worth mentioning, although the following list is by no means all inclusive. Each layer of a network requires specific protocols, which must then work together to make sure that data flow from the sender to the receiver.

- *Ethernet* is the most popular local area network (LAN) technology in use today, both in health care and in business. Ethernet is specified as an IEEE standard (802.3). It was originally developed as a joint effort by several prominent vendors: Xerox, Digital Equipment Corporation, and Intel. Ethernet systems are offered by many different network vendors and come in a variety of *speeds*. 10-BASE-T Ethernet provides transmission speeds of up to 10 Megabits per second (Mbps), Fast Ethernet provides up to 100 Mbps, and Gigabit Ethernet provides up to 1,000 Mbps. (We will discuss transmission speed a little later in this section.)
- *Asynchronous Transfer Mode* (ATM) is a switching technology protocol designed to be implemented with hardware devices allowing faster transmission speeds—up to 10 Gbps.
- *Bluetooth* is a developing communication standard that was first introduced in 1994. It is designed to support communications among cellular phones, handheld computers, and other wireless devices. Health care organizations might employ Bluetooth technology in wireless keyboards, mice, headsets, or PDAs.
- *IEEE 802.11* standards apply to wireless Ethernet LAN technology. Standard 802.11a applies to wireless ATM systems and high-speed switching devices. Standards 802.11b and 802.11g, or Wi-Fi specifications, are used by wireless phones and laptop computers. Standard 802.11g is a newer standard that offers higher speeds and improved performance over 802.11b. Wi-Fi and Bluetooth have been seen as competing standards (WhatIs?com, 2002; Stair & Reynolds, 2003). Wi-Fi is, however, emerging as the more popular standard.

Network Types and Configurations

Computer networks used in health care and elsewhere are described with a variety of terms. In this section you will be introduced to many of these terms. Again, this is not an exhaustive list. As you read these sections, keep in mind that a computer network is a collection of devices (sometimes called *nodes*) that are connected to one another for the purpose of transmitting data. A *network operating system* (NOS) is a special type of system software that controls the devices on a network and allows the devices to communicate with one another. Some of the most common network operating systems on the market today are Microsoft's Windows NT and Windows 2000/2002, and NetWare from Novell (Stair & Reynolds, 2003).

LAN Versus WAN. The first distinction that is often made when describing a network is to identify it as either a *local area network* (LAN) or a *wide area network* (WAN.) LANs typically operate within a building or sometimes across several buildings belonging to a single organization and located in the same general vicinity. The actual distance a LAN covers can vary greatly. One common way to distinguish a LAN from a WAN is that the LAN will have its network hardware and software under the control of a single organization. As the Internet and its related technologies are used more, the line between LANs and WANs may be somewhat blurred. For our purposes, we will think of the LAN as being confined to a single geographical area and controlled by a single organization. A WAN is any network that extends beyond the LAN. WANs can be public (like the Internet) or private. They may be connected by dedicated lines, a satellite, or other media.

The devices and computers that are a part of a LAN will each have a *network interface card* (NIC). These cards are generally specific to the type of LAN transmission technology being employed, such as Ethernet. (This is why you may hear the term *Ethernet card* used to refer to your computer's NIC.) Computers that connect via modems to the Internet may not require the use of NICs. Clearly, most health care organizations today operate one or more LANs and use WANs as well.

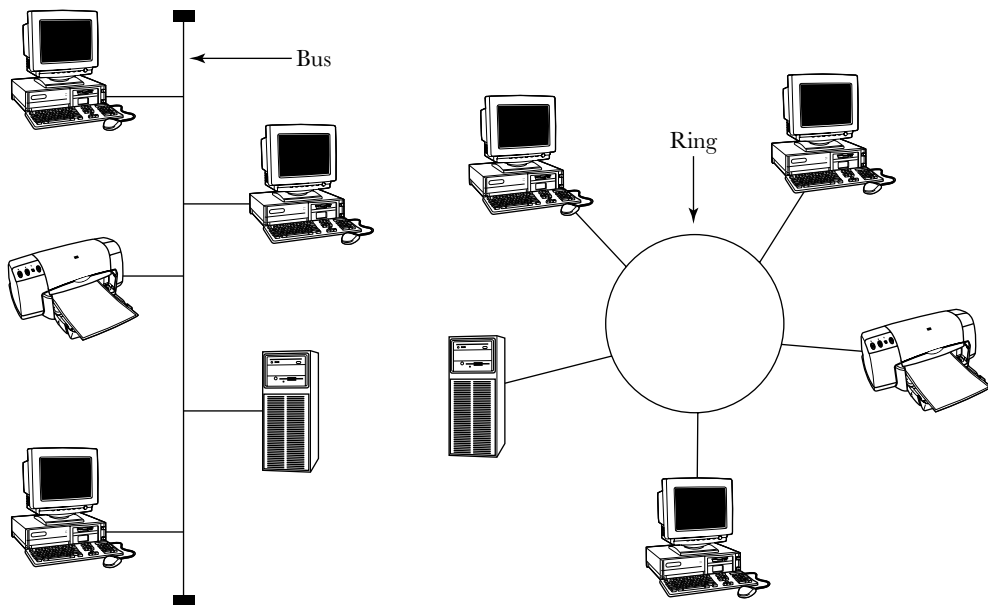
Topology. A second way that networks are described is by their *topology*, or layout. There are two types of network topology: *physical* and *logical*. The physical topology is how the wires are physically configured. The logical topology is the way data flow from node to node in the network. Various arrangements and standards dictate this movement. The two most common logical network topologies, *bus* and *ring*, are depicted graphically in Figure 8.7.

Ethernet employs a bus topology, so this topology is the one most commonly found in health care networks. The bus topology in its simplest form consists of computers and other devices operating along a single *line*. This arrangement allows each device on the network to communicate directly with any other device on the network, without having to pass through interim devices or nodes. It is called a *bus* topology because the data signals travel up and down the single line (like buses on a commuter bus line) until they reach their designation.

IBM Token Ring is an example of a network that employs a logical ring topology. In this type of network a *token*, which is a special bit pattern, travels around in a circular fashion. "To send a message, a computer [or device on the network node] catches the token, attaches a message to it, and then lets it continue to travel around the network" (Webopedia, 2004c).

Physical topology refers to the manner in which the network cables are arranged, in a bus, ring, or *star* arrangement. The two networks presented here as examples of

FIGURE 8.7. BUS AND RING TOPOLOGIES.



logical bus and logical ring networks, Ethernet and IBM Token Ring, are commonly physically configured in a star arrangement. A physical star is depicted schematically in Figure 8.8. Figure 8.9 shows an Ethernet network, which is a logical bus, in a physical star layout. Note that the wiring from the various computer devices on the network comes together in another device, which is called a *hub*.

Network Media and Bandwidth

Two frequently discussed aspects of a network are its media and its bandwidth. *Media* refers to the physical “wires” or other transmission devices used on the network. *Bandwidth* is a measure of media capacity.

Media. Data may be transmitted on a network through several types of media. Common types of conducted media for LANs include *twisted pair wire*, *coaxial cable*, and *fiber-optic cable*. Common wireless media include *terrestrial* and *satellite microwave transmissions*.

FIGURE 8.8. PHYSICAL STAR TOPOLOGY.

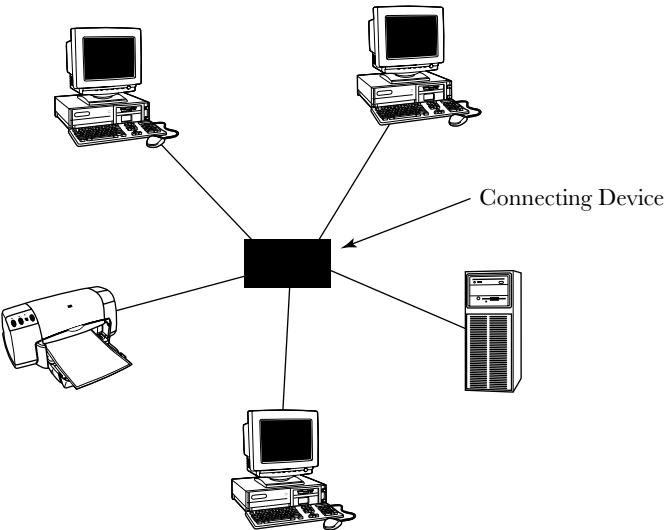
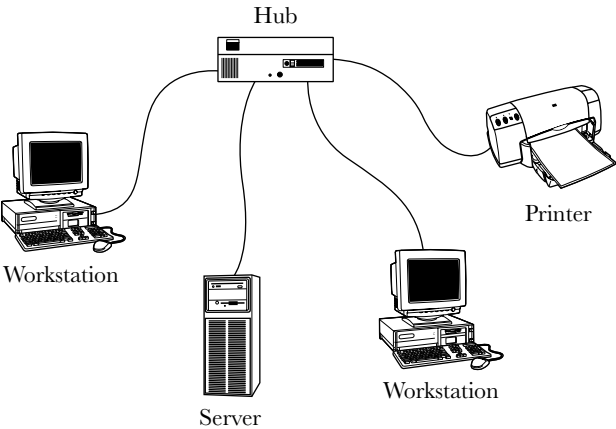


FIGURE 8.9. ETHERNET NETWORK IN A PHYSICAL STAR.



as well as *spread spectrum radio transmissions*. Mobile phone technology and infrared technology are also being used for wireless computer data transmission (White, 2001).

Twisted pair. Twisted pair wire comes in categories, ranging from the “slowest,” Category 1, to the “fastest,” Category 7 (Categories 6 and 7 are currently considered developing technologies, with draft standards). Traditional telephone wire is Category 1 twisted pair. Typical LAN wire is Category 5 or 5e.

Coaxial cable. Coaxial cable is the cable used to transmit cable television signals. The use of coaxial cable in LANs has decreased in recent years due to the availability of high-quality twisted pair and fiber-optic cable.

Fiber-optic cable. Fiber-optic cable is made of thin glass fibers only a little bigger in diameter than a human hair. These glass “wires” are encased in insulation and plastic. The big advantage of fiber-optic cable is its ability to transmit data over longer distances than traditional twisted pair. However, fiber-optic cable is more expensive to use.

Microwaves. Microwaves are a type of radio wave with very short wave lengths. Terrestrial microwave transmission occurs between two microwave antennae. In order to receive and send microwave signals, the sending and receiving antennae must be in sight of one another. Satellite microwave transmission sends microwave signals from an antenna on the ground to an orbiting satellite and then back to another antenna on the ground.

Spread spectrum. Spread spectrum wireless transmission uses another type of radio wave. Unlike conventional radio broadcasting, which uses a specific, consistent wave frequency, spread spectrum technology employs a deliberately varied signal, resulting in greater bandwidth. The popular Wi-Fi (802.11) standard for wireless computing is based on spread spectrum technology (Whatis?com, 2002).

Service Carriers. Communications across a WAN may involve some type of carrier. These telecommunications carriers provide telephone lines, satellites, modems, and other services that allow data to be transmitted across distances. Telecommunications carriers can be either *common carriers*, primarily the long-distance telephone companies, or *special-purpose carriers*. Common carriers can provide either a traditional *switched line*, sometimes referred to as *plain old telephone service* (POTS), or a *dedicated* or *leased line*, which offers a permanent connection between two locations. Telephone companies also offer *integrated services digital network* (ISDN) services. ISDN uses existing phone lines to transmit not only voice but also video and image data in digital form. A purchased *T-1* line is another option for transmitting integrated voice, data, and images for large health care organizations, depending on their needs.

Bandwidth. *Bandwidth* is another name for the capacity of a transmission medium. Generally, the greater the capacity, or bandwidth, of the medium the greater the speed

of transmission. Multiple factors influence transmission speed, and bandwidth is only one of them, but a low bandwidth can impede transmission rates across the network. Transmission rates are expressed as *bits per second* (bps). In other words, a medium's capacity is determined by the maximum number of bps it can carry. Category 1 twisted pair wire has a relatively low transmission speed, 56 Kbps typically, whereas satellite microwave can have speeds exceeding 200 Gbps (Oz, 2004). With some media, a signal that must travel a long distance may have to be enhanced along the way in order to maintain its speed of transmission. Devices that accomplish this task are called *repeaters*.

Network Communication Devices

If you think about how computers are used in the health care organization today, they rarely depend on a single LAN to access all the information needed. At the least a computer will be connected to one LAN and the Internet. Often a single computer in a health care organization will be connected to multiple LANs and several WANs, including the Internet. LANs employ combinations of software and hardware in order to communicate with other networks.

There are several types of devices that allow networks to communicate with another. We will describe a few of the common devices in this section, including *hubs*, *bridges*, *routers*, *gateways*, and *switches*.

Hub. As its name implies, a hub is a device in which data from a network come together. On a schematic, a hub may appear as the "box" where all the Ethernet lines come together for a LAN or a segment of the LAN. Today single devices may serve as hubs and switches or even routers (WhatIs?com, 2002).

Bridge. A bridge connects networks that use the same communication protocol. In the OSI reference model (Figure 8.5), a bridge operates at the data link layer, which is fairly low in the model, which means that it cannot translate signals between networks using different protocols.

Router. A router operates at a higher level, the network layer of the OSI model. Routers are more sophisticated devices than bridges. Whereas bridges send on all data they receive, routers are able to help determine the actual destination of specific data.

Gateway. A gateway can connect networks that have different communication protocols. These devices operate at the transport level of the OSI model, or higher.

Switch. A switch may either be a gateway or a router. In other words, it may operate at the router level or at a higher level. There are many types of switches available on the market today. All switches will route, or *switch*, data to their destination (Stair & Reynolds, 2003).

Information Processing Distribution Schemes

Networks and databases are often described in terms of the method through which the organization distributes their information processing. Three common distribution methods are *terminal-to-host*, *file server*, and *client/server*. All three types are found in health care information networks. A single health care organization may in fact employ one, two, or all three methods of processing distribution, depending on its computing needs and its strategic decisions regarding architecture.

In *terminal-to-host* schemes the application and database reside on a host computer, and the user interacts with the computer using a *dumb terminal*, which is a workstation with no processing power. In some terminal-to-host setups the user may interact with the host computer from his or her personal computer (which obviously has computing power), but special software, called *terminal emulation* software, is used to make the PC act as if it were a dumb terminal when connecting to a specified host computer. *Thin client* schemes are a variation of the host-to-terminal type. The major advantage cited for using this type of distribution is the centralized control. The individuals who support the network and databases no longer have to worry about PC maintenance or how the user might inadvertently modify the configuration of the workstation.

File server systems have the application and database on a single computer. However, the end-user's workstation runs the database management system. When the user needs the data that reside on the file server, the file server will send the entire file to the computer requesting it.

Client/server systems differs from traditional file server systems, in that they have multiple servers, each of which is dedicated to one or more specialized functions. For example, servers may be dedicated to database management, printing, or other program execution. The servers are accessible from other computers in the network, either all computers in the network or a designated subset. The client side of the network usually runs the applications and sends requests from the applications to the server side, which returns the requested data.

The Internet, Intranet, and Extranets

Think of how health care organizations use the Internet today. They maintain informational Web pages for patients, providers, and insurers. They use Internet technologies to facilitate communications and transactions internally and with suppliers and customers. Some health care organizations have developed health information Web applications or have contracted with third parties to maintain patient records electronically. Telemedicine and *electronic data interchange* (EDI) functions may be Web-based. The

list of examples goes on. This is truly an amazing phenomenon when you consider that the vast majority of this Internet and Web application development has occurred in the last decade. Although the Internet has its early roots in an effort that began in the late 1960s, it was not until the development of the World Wide Web (WWW) that businesses, including health care organizations, began to see the benefit of on-line communications and on-line business transactions (e-commerce). Internet use is one of the most rapidly growing aspects of health information technology. In this section we will examine the technologies that make Web-based e-commerce possible for health care organizations. We will describe the fundamentals of Internet and WWW technologies and explore a few of the more recent developments.

The Internet

What, exactly, is the Internet? The image that today's user has of the Internet is the multimedia world of the WWW; however, this is only one part of the vast network of networks known as the Internet. The WWW is the means by which the majority of users interact with the Internet, but the WWW and the Internet are not the same.

The Internet began in 1969 as a government project to improve defense communications. This precursor to today's Internet was known as the Advanced Research Projects Agency Network (ARPANET). The goal of the Advanced Research Projects Agency was to establish a network that could survive a nuclear strike; therefore it was intentionally developed without a central point of control. This is a characteristic of the Internet that still exists today. Believe it or not, ARPANET began as a network of four computers. In the beginning ARPANET was open only to academic institutions and portions of the national defense infrastructure. As it grew, the network divided into a civilian and a government branch. The civilian branch became known as the Internet. In 1991, the government decided to allow businesses to link to the Internet, but not many businesses were interested in this until the WWW was introduced a couple of years later. The WWW is what brought multimedia and ease of use to the Internet and its applications. Since the introduction of the WWW, Internet use among all types of businesses (including health care) has exploded.

The *backbone* of the Internet today is owned and maintained by multiple organizations in many countries. The Internet backbone is made up of many high-speed networks linked together. These networks use multiple types of communication media, such as optical fiber, satellite, and microwave transmission. Think of the components of this backbone as the major highways of the Internet. The Internet, like its predecessor, ARPANET, has no single point of control. Specific segments of the Internet backbone are owned and maintained by telecommunications companies and Internet service providers (ISPs), such as Sprint, MCI, Verizon, and America Online (AOL), to name just a few (Oz, 2004; Stair & Reynolds, 2003; Whatis?com, 2002).

How the Internet Works. Every computer and device that operates within the Internet has a unique identifier known as an *Internet Protocol* (IP) number, or address. Specific Internet protocols (discussed early in this chapter) allow each computer or device on the Internet to use these IP addresses to locate other computers or devices. The IP address is a four-part number, with each part separated by a period. All Web sites have an IP address; however, most are also associated with a character-based address that is easier for people to remember. The process of associating the numerical IP address with the character-based name is accomplished by a *Domain Name System* (DNS) server, which is maintained by an ISP. IP addresses may be static or dynamic. Static addresses are permanently assigned to a computer or device. A dynamic address is assigned “as needed” by a special server that recognizes when a computer or device needs an address. Dynamic IP addressing gives an organization flexibility in using its allotted IP addresses.

Blocks of IP addresses are assigned to organizations by one of several domain name registrars. Again, remember that one of the hallmarks of the Internet is the absence of a central point of control. The companies that register domain names and IP addresses are for-profit organizations that sell their name registration services. There is also one database that contains all domain names, IP addresses, and “owners”; it is maintained by Network Solutions, Inc. (Oz, 2004; Stair & Reynolds, 2003; Whatis?com, 2002).

World Wide Web. The use of the Internet changed dramatically when a British scientist invented the software protocol *Hypertext Transfer Protocol* (HTTP). HTTP allows full-color graphics, tables, forms, video, and animation to be shared over the Internet. The code used for displaying files on the WWW is called a *markup language*. The most common markup language today is HTML (*hypertext markup language*). HTML defines how pages look on the Web by using *tags*, special codes that inform a Web browser how text or other content should look. A newer markup language that many think will change the way data is captured and stored is the *extensible markup language* (XML). Unlike HTML, which defines only how pages look, XML also defines what the data enclosed in the tags *are*. XML holds a lot of promise as a messaging standard in health care applications. Figure 8.10 presents examples of HTML and XML code.

Think about using the WWW. How do you get to the Web page you want? Typically, you type the URL (*uniform resource locator*) for the page (for example, <http://www.musc.edu/chp/facstaff.htm>) into an application known as a *Web browser*. The best-known Web browsers are Internet Explorer and Netscape. However, interest is increasing in the open-source browser Mozilla. Browser software allows Web users to search for and retrieve specific Web sites. Today, browsers also allow the user to use additional software components, known as *plug-ins*, to perform functions such as viewing videos or listening to audio.

FIGURE 8.10. XML AND HTML CODE.

XML

```
<patient>
<patient.id>12345</patient.id>
<patient.name>John Doe</patient.name>
<patient.date.of.birth>November 21, 1953</patient.date.of.birth>
</patient>
```

Tags define the actual data elements.

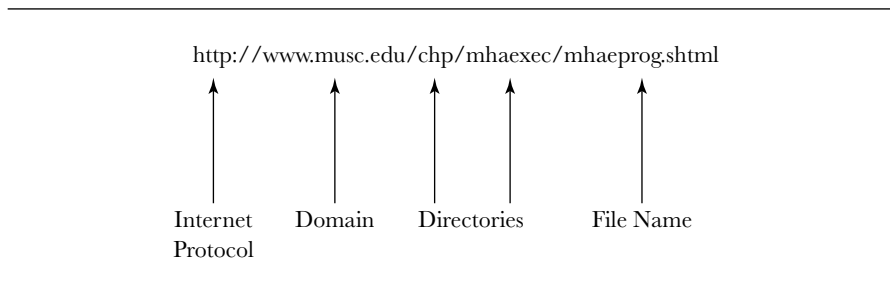
HTML

```
<p>MRN: 12345<br>
Name: John Doe<br>
Date of Birth: November 21, 1953</p>
```

Tags define how the text will look and not the data the text represents.

Figure 8.11 shows the various components of a URL. The HTTP part of the address indicates that Hypertext Transfer Protocol is being used. HTTP is one of the protocols that make up TCP/IP. (Another TCP/IP protocol, HTTPS, is a secure variation of HTTP that employs encryption to protect the site.) The next component, *www.musc.edu*, is the *domain name* (a domain name may or may not include *www*). The *edu* section of the address in Figure 8.11 is the *top-level domain* (TLD), which often indicates the type of organization that registered the domain name. Some TLDs, such as *edu*, *mil*, and *gov* are restricted to use by qualified organizations. However, some, such as *com*, *org*, and *net* are less restricted and can be used by any individual or organization in the appropriate generic category. The next section of the URL indicates the specific directory, or folder, where the Web page resides. In our example there are two directories, but there could be several or only one. The final component of the URL is the actual name of the file to be located. In this example the file ends with the extension *shtml*, which shows that it was created, or coded, using a specific version of HTML (Oz, 2004; Stair & Reynolds, 2003; Whais?com, 2002).

Other Internet Applications. As mentioned earlier, most of us associate the Internet with the WWW, but Web browsers are not the only Internet applications that are used by health care organizations. Some other common applications are e-mail, file transfer, and Internet telephoning.

FIGURE 8.11. URL COMPONENTS.

E-mail. E-mail is one of the most popular uses of the Internet. The TCP/IP set of protocols include e-mail protocols that allow point-to-point text-based communications. The basic form of e-mail is encoded text, but graphic and sound files can be sent as attachments. The most common protocol for outgoing e-mail is *Simple Mail Transfer Protocol* (SMTP). *Post Office Protocol 3* (POP3) and *Internet Message Access Protocol* (IMAP) are common protocols for receiving mail (Whatis?com, 2002).

File transfer. *File Transfer Protocol* (FTP) is the TCP/IP protocol that allows point-to-point transfer of files from one computer to another. FTP is incorporated into Web sites and e-mail to allow the downloading of files. Files transferred using FTP can be text, graphics, animation, or sound files.

Internet telephoning. Internet telephoning is gaining popularity in the business community and in health care organizations. The protocol that allows Internet telephoning is *Voice over Internet Protocol* (VoIP). Organizations that want to use Internet telephoning must have the appropriate software and microphones attached to computers. They must either purchase software or use a company that provides Internet telephone services. As this technology continues to improve over time, organizations are finding it to be a viable, and less expensive, option to traditional long distance. According to one estimate, the cost of a VoIP telephone conference will be about 25 percent that of a traditional telephone conference (Oz, 2004).

Intranets and Extranets

An *intranet* is a computer network that is internal to an organization and that uses Internet technologies. Intranets can be used for virtually any type of internal network application. The network designers develop Web applications that are accessible via Web browsers. Although an intranet uses both “public” Internet routes and internal network lines, it is generally a secure network that is protected from outside users. For example, a hospital may set up an intranet site with employee benefits and forms that can be accessed only from authorized computers within the organization or by

employees entering the organization's network through a secure mechanism. The secure path established between the Internet and an intranet, using a combination of software and hardware protections, is sometimes referred to as a *tunnel*.

An *extranet* is similar to an intranet except that the network of users includes business partners of the health care organization, such as suppliers, customers, or other health care providers. Again, extranets are generally secure, limiting access to their sites (Oz, 2004).

Clinical and Managerial Decision Support

Health care executives and providers are faced with decisions every day, multiple times per day. The success of any health care organization literally depends on these large and small decisions. In this section we will describe technologies that support decision making in health care today, for both clinical and managerial decision. The types of systems that we will examine are

- Decision-support systems (DSS)
- Artificial intelligence systems, including expert systems, natural language processing, fuzzy logic, and neural networks

Nobel Prize-winning economist Herbert Simon described decision making as a three-step process (Oz, 2004; Stair & Reynolds, 2003):

1. Intelligence: collecting facts, beliefs, and ideas. In health care these facts may be stored as data elements in a variety of data stores.
2. Design: designing the methods with which to consider the data collected during intelligence. These methods may be models, formulas, algorithms, or other analytical tools. Methods are selected that will reduce the number of viable alternatives.
3. Choice: making the most promising choice from the limited set of alternatives.

Problems that face health care executives and clinicians may be *structured*, *unstructured*, or *semistructured*. Structured problems are also referred to as *programmable* problems, because a computer program can be written with relative ease to solve this kind of problem. Transaction-based applications can be used to solve structured, or programmable, problems. For example, a payroll system is based on known facts about each employee's salary, deductions, and so on. The "decision" of how much to write the monthly paycheck for is fairly straightforward. The unstructured and semistructured problems present much more of a challenge for computer application developers.

Decision-Support Systems

How do we harness the power of a computer to solve a problem or make a decision about a solution when the situation is not easily structured with a simple algorithm (sequence of logical steps)? The computer systems developed to tackle the unstructured or semistructured problem are called *decision-support systems* (DSS). *Decision-support system* is another term that can mean slightly different things to different vendors or users. In this section we are referring primarily to the traditional, stand-alone DSS: in other words an application that is designed for the purpose of supporting decisions. This is not the only form of decision support available to health care executives and providers today. For example, patient care or administrative applications may have components, such as data mining, that aid in decision making, but these applications might not be classified as full-blown DSS. An electronic spreadsheet, such as Excel, can also be used as a decision-support tool. Spreadsheets have built-in functions as well as the ability to use “what if” statements.

The stand-alone DSS generally has three distinct components:

- The data management module, which is an existing or built-in transactional database or data warehouse. In a clinical DSS, the data module could be a clinical data repository.
- The model management module, which allows the user to select a model to be applied to the problem at hand. Models can be mathematical, statistical, or based on expert knowledge. The model management module of a DSS is its most complex component and may seem like a “black box” to the health care executive.
- The dialog module, which is the user interface. This module allows the user to pose the problem to the system by selecting the data and the decision model to use on the data. The dialog module also displays results, generally in text and graphical formats.

Executive information systems (EIS) are decision-support systems specifically designed for the higher-level manager. Most of these systems have drill-down capability to allow the executive to examine a problem at different levels of granularity, and many are tied to data warehouses (Oz, 2004).

Artificial Intelligence

Artificial intelligence (AI) is a branch of computer science that is devoted to emulating the human mind. One very common use of AI today is incorporated into the Google search engine. When the user types a misspelled word in a string of keywords, Google will suggest alternative key words based on the context of the query (Oz, 2004). AI is a broad field with many different types of technology. Most AI is quite complex

and describing the underlying technology is beyond the scope of this text. However, we will introduce a few types of AI that may be found in health care settings.

Expert Systems. The hallmark of expert systems is that they use heuristics, or “rules of thumb,” that are collected from experts in the particular field for which the system was built. Expert systems comprise

- A knowledge base, which stores all the relevant information, data, rules, and cases that will be used by the system. It is similar to a database, but the relationships are designed to match those dictated by the human experts. One of the challenges of building the knowledge base is getting the expert knowledge. Experts, being people, do not always agree on the way to approach a problem.
- An inference engine, which provides the expert advice from the knowledge base.
- An explanation facility, which allows the user to understand how the inference engine arrived at the advice it is presenting.
- A knowledge acquisition facility, which allows the user to update the knowledge base with new or additional expert information (Stair & Reynolds, 2003).

Natural Language Processing. Natural language processing (NLP) programs take human language (typed as text or input as voice) and translate it into a standard computer instructions, such as SQL. Suppose you typed this text into an application:

List the names of all drugs that will treat shingles for less than \$60 per month.

Or:

What are the names of the drugs that will treat shingles for less than \$60 per month?

A NLP program might recognize this sentence in context and convert it to an SQL statement similar to this:

```
SELECT NAME FROM DRUGS
WHERE DISEASE = "SHINGLES"
AND COST < 60
```

So far NLP programs have met with limited success. The difficulty is in identifying all of the possible meanings of words or combination of words based on context. This problem is magnified in the health care community by medical terminology that is both complex and seems to be ever-changing.

Neural Networks. *Neural networks* or *neural nets* may be used by sophisticated expert systems. They are software programs that attempt to mimic the way the human brain operates. This is in contrast to the traditional, step-by-step process used in other computer programming languages. Neural networks involve a very sophisticated level of programming, but they are employed in both business and health care applications today.

Fuzzy Logic. *Fuzzy logic* is based on rules that may have overlapping boundaries. This logic is designed to help the expert system deal with ambiguity and uncertainty (Oz, 2004).

Trends in User Interactions with Systems

This section of this technology chapter is devoted to describing some of the new and not-so-new devices that enhance the user interface with the health care information system. There have been many developments in input and output devices, along with personal computing devices, in the past few years. These developments are likely to continue and will affect the way in which users expect to interact with health information systems. The list of devices discussed in this section is by no means all inclusive. Each coming year will likely see new or improved devices on the market. However, these discussions will give you an overview of the various types of devices that are available at the time of this writing. We examine four categories of devices:

- Input devices
- Output devices
- External storage devices
- Mobile personal computing devices

Input Devices

The most common computer input devices in use today are the standard keyboard and the mouse. These devices have undergone a few changes since their introduction with personal computers, such as ergonomic improvements in shape and size and the addition of wireless technologies. Both the keyboard and the mouse are now available in wireless forms, which employ infrared or radio-frequency technologies.

Other commonly used input devices and methods include trackballs, trackpads, touch screens, source data input devices such as bar-code scanners, and systems for imaging and speech recognition. *Trackballs* and *trackpads* work like the standard mouse. The computer detects the movements of the ball or the user's touch on the pad and translates them into digital coordinates on the computer screen. *Touch screens* (Figure 8.12)

FIGURE 8.12. TOUCH SCREEN.

Source: Courtesy of MUSC.

allow the user to choose operations by touching the surface of the computer screen. The technology of touch screens comes in two basic forms. In one, the pressure of the touch results in an electrical contact between two layers of the screen, causing an electrical current to move through the screen to a sensing device. In the other, acoustical waves are converted to electrical signals. Touch screens are used in handheld computing devices as well as in PCs (Oz, 2004; Stair & Reynolds, 2003).

A special class of input devices known as *source data input devices* includes optical mark recognition, optical character recognition, and bar-coding devices, among others. Although *bar coding* has been commonplace in retail venues for many years, it has recently received a lot of attention in the health care community as a means of improving patient safety. *Optical bar-code recognition* devices recognize data encoded as a series of

thick and thin *bars*. As with other technologies, the success of bar codes in health care stems from the development of standards, in this case the Health Industry Bar Code (HIBC) standard. The HIBC standard was developed for applications such as medical product and drug identification and device tracking. It is approved by ANSI (a standards-governing organization discussed in the next chapter) and administered by the Health Industry Business Communications Council (HIBCC). The standard specifies a primary label and an optional secondary label. The primary label bar code includes the labeler's unique identification code, the product or catalogue number, and the packaging level. The secondary label bar code allows the inclusion of such data as expiration date, lot number, quantity, batch number, and serial number, which are important when dealing with medical products and devices (Hankin, 2002). As mentioned in Chapter Five, a common health care use of bar coding is in medication administration systems that employ barcode-enabled point of care (BPOC) functions.

Many health care organizations have looked to *document imaging systems* as a means of getting data into health care information systems. Document imaging systems scan documents and convert them to digital images. These images are then stored in databases for later retrieval. The disadvantage of imaging systems is that they require a great deal of storage capacity, but their greatest advantage is that a digitized document, such as a patient record, is available to multiple users simultaneously. With the availability of inexpensive, high-capacity storage media, such as compact disks (CDs) and digital video disks (DVDs), imaging systems became feasible alternatives for integrating documents into health care information systems. Think back to our discussion of the Medical Records Institute's levels of automation and computerization of medical records; Level 2 systems rely on this form of imaging.

Speech recognition, or *voice recognition*, is another input method used in health care. It is particularly suited for situations or work environments where using a keyboard, mouse, or touch screen is not practical, such as the pathology lab or surgical suite. Speech recognition systems today vary in level of sophistication. The simplest systems are designed to "learn" a person's speech pattern. A user speaks into a microphone, and the speech recognition software learns the particular intonations, vocabulary, and patterns associated with that user. Once the user's speech pattern is learned, the voice is converted to computer-readable data. The disadvantage of these systems is the time it takes to "train" the computer to recognize the speech. This is a particular challenge in an area with many users. Higher-end systems are designed to understand any person's speech, but most of these systems have fairly limited built-in vocabularies. Most would agree that speech recognition is still under development and its use is most likely in certain segments of health care, such as radiology, pathology, and emergency medicine. However, it does have the potential to be used with many other types health care applications. An example of a voice recognition system marketed to health care providers is Dragon Naturally Speaking Medical Solutions (Oz, 2004).

Output Devices

The most commonly used computer output devices are the computer monitor and the printer. There are two basic types of monitors: traditional monitors that use *cathode ray tube* (CRT) technology and flat panel monitors, such as those that use *liquid crystal display* (LCD) technology. Notebook and handheld computing devices rely on flat screen technology, and they have also become a popular alternative to the CRT for desktop computers. Printers are either *impact* or *nonimpact*. Nonimpact printers use laser, ink jet, electrostatic, and electrothermal methodologies. They print without a print head that touches the paper. They can produce a very high-quality printed document. Impact printers include dot matrix printers, in which pins strike a printer ribbon to make the print. Impact printers have become less popular as the cost of nonimpact printers has dropped considerably.

Speech output is another form of computer output that is becoming more common place. Automated telephone answering systems employ computer speech output, for example. There are two approaches to speech output: in one, phrases prerecorded by a person are strung together to form the output desired; in the other, synthesized speech, a machine produces speech sounds (Oz, 2004).

External Storage Devices

Health care information systems require the extensive use of external storage devices. Critical systems must be backed up regularly, and data must be frequently archived for permanent or nearly permanent storage. What are some of the options available for external storage of computer data? There are two basic types of storage media, *sequential* and *direct access*.

In sequential storage, data are stored one record after another, in some logical order, such as by patient identification number or date. When the computer is asked to locate a record, it must read through all the stored data that precede the record it is seeking. This makes retrieval from sequential storage slower than retrieval from direct access devices. Magnetic tape is the most common sequential storage medium. Data are stored as magnetic *spots*, or points, on magnetic tapes. The data are then read via a device called a *tape drive*. Magnetic tapes are inexpensive and frequently are used to store large amounts of backup data.

Direct access storage media allow the data of interest to be accessed without first going through previously stored data. Common forms of direct access storage media are magnetic disks (including external hard drives), floppy disks, and zip drives. Information is coded in a manner similar to that used for magnetic tape, with magnetized spots, or points, on the disk surface. Data are read by a compatible *disk drive*. A special form of disk technology called *redundant array of independent disks* (RAID) can be

used by health care organizations to protect their information by creating redundancy: in other words, they can still reproduce data even if one disk fails. RAID systems have groups of hard disks, which can number in the hundreds, controlled through a software application. RAID systems come in a variety of capacity levels, but all are designed to enable data restoration in a timely manner (Oz, 2004).

Among the newer types of external storage is optical disk technology, which is available in such forms as *compact disks* (CDs), *digital video disks* (DVDs), and *optical tape*. The technology behind optical storage media is that the medium's surface is altered by a laser so that it reflects light in two different ways. These two ways are then interpreted by the computer as the 1s and 0s needed for digitizing. CDs come in several forms, read only memory (CD-ROM), recordable (CD-R), and rewritable (CD-RW). CDs are less expensive than magnetic storage media and they can hold more data per surface area. Newer CD drives allow CD users to read, write, edit, and delete data as they would on a magnetic disk. DVDs hold even more data than CDs and are particularly well suited for storing multimedia. Personal computers now come equipped with drives that will read and write to both DVDs and CDs. Optical tape uses the same technology as optical disks, but data are stored sequentially and the storage capacity is very large (one cassette can hold about nine gigabytes of data) (Oz, 2004; Stair & Reynolds, 2003).

Flash memory is another form of external storage (and internal storage in many handheld computer devices) that is gaining popularity as its costs come down. Flash memory consists of a computer memory chip that can be rewritten and does not lose its data when the power source is removed. Removable flash memory devices take several forms, but one of the most popular is a *thumb drive* (Figure 8.13). This device plugs into an USB port and can provide over 2 GB of memory. Compared to other external storage, flash memory can be accessed more rapidly, consumes less power, and is smaller in size. The disadvantage is its comparative cost (Oz, 2004; Stair & Reynolds, 2003).

Mobile Personal Computing Devices

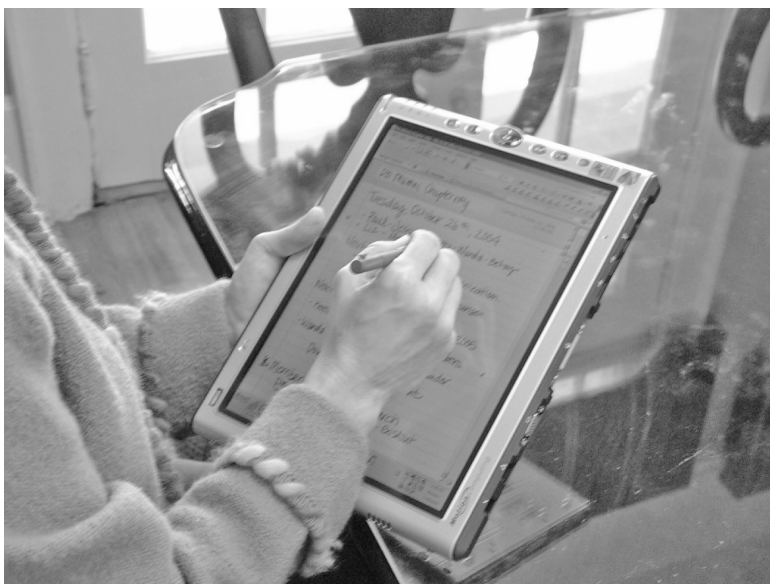
Many types of mobile personal computing and handheld devices are used in health care today. In fact many health care organizations have had to respond to providers who have adopted *personal digital assistants* (PDAs) and *pocket PCs* and who subsequently want and expect to be able to access health care applications from these devices. In this section we will look at several types of personal computing devices, including laptop computers, tablet computers, PDAs, and so-called smart phones. All of these devices have one thing in common—they are portable and all are wireless or, in the case of laptop computers, can be wireless. This feature creates special security issues for health care organizations (discussed in more detail in Chapter Ten). The use of mobile devices to access sensitive health care data must be addressed and ultimately controlled.

FIGURE 8.13. THUMB DRIVE.

A *laptop* (or *notebook*) computer (Figure 8.14) is a compact, lightweight personal computer. The screen and keyboard are built in. Although they still lag somewhat behind desktop computers in speed, memory, and capacity, today's laptops are powerful enough to replace traditional desktop computers. The *tablet* computer (Figure 8.15) is a relative new comer to the PC market. It was introduced by Microsoft in 2001. It is a full-power PC that is the size of a thick writing tablet. Although the tablet computer can be connected to a mouse and keyboard, the user may instead use a stylus to navigate (Oz, 2004). This increases the mobility of the tablet computer. Laptops and tablet computers are being adopted by health care organizations for point-of-care or bedside systems.

FIGURE 8.14. LAPTOP COMPUTER.

**FIGURE 8.15. TABLET COMPUTER.**



*PDA*s began to be marketed to the general public in the early 1990s. Since that time their use has steadily increased. *PDA*s (Figure 8.16) generally use a stylus for data input and most can recognize handwriting to some extent (though not yet perfectly) (Oz, 2004). Newer *PDA*s allow users not only to store data, such as calendars and personal notes, but also to connect to the Internet to browse Web pages and send or receive e-mail. These devices are becoming more powerful and less expensive, which will likely increase their popularity. More software applications are being developed specifically for *PDA*s. In the health care community, resources such as medical dictionaries, formularies, and clinical coding systems can be installed on *PDA*s.

As *PDA*s and cellular phones both gained popularity, the market recognized the potential for incorporating aspects of both into a single device, sometimes called a *smart phone*. These devices are evolving rapidly, and we will likely see them employed in health care organizations.

FIGURE 8.16. PERSONAL DIGITAL ASSISTANT.



Information Systems Architecture

In the preceding sections we introduced many specific technologies that can be used in health care organizations. However, a huge question remains: How does the organization choose among these technologies and ultimately bring them together into a cohesive set of health care information systems? This section answers these questions by examining health care information system architecture.

An organization's information systems require that a series of core technologies *come together*, or work together as whole, to meet the IT goals of the organization. Up to this point in the chapter we have discussed the core technologies but have not discussed how they work together as a cohesive information system. The way that core technologies, along with the application software, come together should be the result of decisions about what information systems are implemented and used within the organization and how they are implemented and used. For example, the electronic medical record system or the patient accounting system with which users ultimately interact represents not just the application software but also the network, servers, security systems, and so forth that all come together to make the system work effectively. This coming together should never be a haphazard process. It should be engineered.

In discussing health care information system architecture, we will cover several topics:

- A definition of architecture
- Architecture perspectives
- Architecture examples
- Observations about architecture

A Definition of Architecture

A design and a blueprint guide the coming together of a house. The coming together of information systems is guided by information systems *architecture*. For the house, the development of the blueprint and the design is influenced by the builder's objectives for the house (is it to be a single-family house or an apartment building, for example), and the desired properties of the house (energy efficient or handicap accessible, for example). For an organization's information systems, the development of the architecture is influenced by the organization's objectives (electronic medical records that span multiple hospitals, for example) and the systems' desired properties (efficient to support and having a high degree of application integration, for example).

Following the design and the blueprints, the general contractor, plumbers, carpenters, and electricians use building materials to create the house. Following the

architecture for the organization's information systems, the IT staff and the organization's vendors implement the core technologies and application software and integrate them to create the information systems.

Information systems architecture consists of concepts, strategies, and principles that guide an organization's technology choices and the manner in which the organization integrates and manages these choices. For example, an organization's architecture discussion concludes that the organization should use industry standard technology. This decision reflects an organizational belief that standard technology will have a lower risk of obsolescence, be easier to support, and be available from a large number of information technology vendors that use standard technology. Guided by its architecture decision, the organization chooses to implement networks that conform to a specific standard network protocol and decides to use the Windows operating system for its workstations.

Two additional terms are sometimes used either as synonyms for or in describing architecture, *platform* and *infrastructure*. In this text, however, we adhere to accepted distinctions among these three terms. For example, you might hear IT personnel say that "our systems run on a Microsoft, HP, and Cisco platform." *Platforms* are the specific vendors and technologies that an organization chooses for its information systems. You might hear of a Windows platform or Web-based platform. Platform choices should be guided by architecture discussions. You might also hear IT personnel talk about the *infrastructure* of the health care information system. *Infrastructure* as we use it refers primarily to the organization's computer networks and, perhaps, to the applications running on those networks. Although *infrastructure* is not vendor or technology specific, it is not quite as broad a term as *architecture*, which encompasses much more than specific technologies and networks.

Architecture Perspectives

Organizations adopt various frames of reference as they approach the topic of architecture. This section will illustrate two approaches, one based on the characteristics and capabilities of the desired architecture and the other based on application integration.

Characteristics and Capabilities. Glaser (2002, p. 62) defines architecture as "the set of organizational, management, and technical strategies and tactics used to ensure that the organization's information systems have critical, organizationally defined characteristics and capabilities." For example, an organization can decide that it wants an information system that has characteristics such as being agile, efficient to support, and highly reliable. In addition, the organization can decide that its information systems should have capabilities such as being accessible by patients from their homes or

being able to incorporate clinical decision support. If it wants high reliability, it will need to make decisions about fault-tolerant computers and network redundancy. If it wants users to be able to customize their clinical information screens, this will influence its choice of a clinical information system vendor. If it wants providers to be able to structure clinical documentation, it will need to make choices about natural language processing, voice recognition, and templates in its electronic medical record.

Application Integration. Another way of looking at information systems architecture is to look at how applications are integrated across the organization. One often hears vendors talk about architectures such as *best of breed*, *monolithic*, and *visual integration*. Best of breed describes an architecture that allows each department to pick the best application it can find and that then attempts to integrate these applications by means of an interface engine that manages the transfer of data between these applications—for example, it can send a transaction with registration information on a new patient from the admitting system to the laboratory system.

Monolithic describes the architecture of a set of applications that all come from one vendor and that all use a common database management system and common user interface.

Visual integration architecture wraps a common browser user interface around a set of diverse applications. This interface enables the user, for example, a physician, to use one set of screens to access clinical data even though those data may come from several different applications.

This view of architecture is focused on the various approaches to the integration of applications; integration by sharing data between applications, integration by having all applications use one database, and integration by having an integrated access to data. This view does not address other aspects of architecture: for example, the means by which the organization might get information to mobile workers.

Architecture Examples

A few examples will help to illustrate how architecture can guide information technology choices. Each example begins with an architecture statement and then shows some choices about core technologies and applications and the approach to implementing them that might result from this statement.

Statement: We would like to deliver an electronic medical record to our small physician practices that is inexpensive, reliable, and easy to support. To do this we will

- Run the application from our computer room, reducing the need for practice staff to manage their own servers and do tasks such as backups and applying application enhancements.

- Run several practices on one server to reduce the cost.
- Obtain a high-speed network connection, and a backup connection, from our local telephone company to provide good application performance and improve reliability.

Statement: We would like to have decision-support capabilities in our clinical information systems. To do this we will

- Purchase our applications from a vendor whose product includes a very robust rules engine.
- Make sure that the rules engine has the tools necessary to author new decision support and maintain existing clinical logic.
- Ensure that the clinical information systems use a single database with codified clinical data.

Statement: We want all of our systems to be easy and efficient to support. To do this we will

- Adopt industry standard technology, making it easier to hire support staff.
- Implement proven technology, technology that has had most of the bugs worked out.
- Purchase our application systems from one vendor, reducing the support problems and the finger pointing that can occur between vendors when problems arise.

Observations About Architecture

Organizations will often bypass the architecture discussion in their haste to “get the IT show on the road and begin implementing stuff.” Haste makes waste as people say. It is terribly important to have thoughtful architecture discussions. There are many organizations, for example, that never took the time to develop thoughtful plans for integrating applications and that then discovered, after millions of dollars of IT investments, that this oversight meant that they could not integrate these applications or that the integration would be both expensive and limited.

As we will see in Chapter Thirteen, organizations that have been very effective in their applications of IT over many years have had a significant focus on architecture. They have realized that thoughtful approaches to agility, cost efficiency, and reliability have a significant impact on their ability to continue to apply technology to improve organizational performance. For example, information systems that are not agile can be difficult (or impossible) to change as the organization’s needs evolve. This ossification can strangle an organization’s progress. In addition, information systems that have reliability problems can lead an organization to be hesitant to implement

new, strategically important applications—how can they be sure that this new application will not go down too often and impair their operations? In Chapter Twelve, we will discuss planning the system architecture as a component of strategic IT planning.

Organization leadership must take time to engage in the architecture discussion. The health care executive does not need to be involved in deciding which vendor to choose to provide network switches. But he or she does need a basic understanding of the core technologies in order to help guide the formation of the principles and strategies that will direct that decision. In the following example, the application integration perspective on architecture (choosing among best of breed, monolithic, and visual integration) illustrates a typical architecture challenge that a hospital might face.

Perspective: Choosing the System Architecture

A hospital has adopted a best-of-breed approach and, over the course of several years, has implemented separate applications that support the registration, laboratory, pharmacy, and radiology departments and the transcription of operative notes and discharge summaries. An interface engine has been implemented that enables registration transactions to flow from the registration system to the other systems.

However, the physicians and nurses have started to complain. To retrieve a patient's laboratory, pharmacy, and radiology records and transcribed materials, they have to sign into each of these systems, using a separate user name and password. To obtain an overall view of a patient's condition, they have to print out the results from each of these systems and assemble the different printouts. All of this takes too much time, and there are too many passwords to remember.

Moreover, the hospital would like to analyze its care, in an effort to improve care quality, but the current architecture does not include an integrated database of patient results.

The hospital has two emerging architectural objectives that the current architecture cannot meet:

1. Provide an integrated view of a patient's results for caregivers.
2. Efficiently support the analysis of care patterns.

To address these objectives, the hospital decides to implement a browser-based application that

- Gathers clinical data from each application and presents it in a unified view for the caregivers.
- Supports the entry of one user ID and password that is synchronized with the user ID and password for each application.

In addition the hospital decides to implement a database that receives clinical results from each of the applications and stores the data for access by query tools and analysis software.

To achieve its emerging objectives, the hospital has migrated from best-of-breed architecture to visual integration architecture. The hospital has also extended to visual integration architecture by adding an integrated database for analysis purposes.

In analyzing what would be the best architecture to meet its new objectives, the hospital considered monolithic architecture. It could meet its objectives by replacing all applications with one integrated suite of applications from one vendor. However, the hospital decided that this approach would be too expensive and time consuming. Besides, the current applications (laboratory, pharmacy, and radiology) worked well; they just weren't integrated. The monolithic architecture approach to integration was examined and discarded.

Summary

The value of this chapter to the health care executive is that it provides a broad overview of health care information architecture and several categories of specific information technologies. Although these technologies are not unique to health care, health care organizations use them for their information systems. We discussed various technologies used for system software; data management and access; networks and data communications; information processing distribution schemes; the Internet, intranets, and extranets; and clinical and managerial decision support; and we also looked at trends in user interactions with systems.

We ended our discussion with the concept of system architecture, the way in which all the technologies in an organization fit together to support health care applications. Like many fields, IT has its own language. It is helpful for health care executives to learn IT terminology so they can to communicate effectively with IT staff and vendors. The overall goal of this chapter was to provide information to support an understanding of the many components that go into health information systems.

Chapter Eight: Learning Activities

1. Technology is changing and evolving. Conduct a search of the Internet or print literature to identify several new or emerging technologies. Describe each technology, and discuss its potential use in the management of health care information or development of health care information systems.
2. Visit a small health care facility or physician's office. Describe the computer network that is used. Does this location use both a LAN and a WAN? What functions

are limited to the LAN? Which use a WAN? Discuss the topology (physical and logical) of the LAN, the hardware components, and the specific protocols employed. Ask for a copy of the LAN diagram for the office (if one exists) or create one from your visit.

3. Do an Internet search and find at least one site that offers a decision-support product to health care executives. Describe the product. Can you tell from the site whether or not the product employs artificial intelligence? Can you tell which type? How useful would the product be to you as a health care executive?
4. Meet with a CIO, director, or IT manager in a health care organization. Ask him or her to describe the architecture used for the clinical component of the organization's health care information system. Based on this conversation, describe how this IT professional views the architecture. What process did this organization use to determine its architecture design? Does it have plans to move to a different architecture?



CHAPTER NINE

HEALTH CARE INFORMATION SYSTEM STANDARDS

In order to achieve interoperability, portability, and data exchange, health care information systems must employ standards. Systems that conform to different standards cannot communicate with one another. For a simple analogy, think about traveling to a country where you do not speak the language. You would not be able to communicate with that country's citizens without a common language or translator. Think of the common language as the standard to which all parties agree to adhere. Once you and others agree on a common language, you and they can communicate. You may still have some problems, but generally these can be overcome.

A plethora of information technology (IT) standards, including standards for messaging, content and coding, networks, electronic data interchange, and electronic health records, are important to health care information systems. Some of these standards compete with one another. The National Alliance for Health Information Technology (NAHIT), an organization formed to compile health care IT standards, has identified 450 voluntary and mandated standards from 150 organizations (Bazzoli, 2004). It is important to recognize that many IT standards that do not specifically address health care also have a tremendous impact on health care information systems. In Chapter Eight we reviewed basic communication protocols and extensible markup language (XML), which is emerging as a messaging standard not only in business-related Internet transactions but also in health care transactions and communications. In discussing system software we mentioned the emergence of Linux, and in examining data management we commented on structured query language (SQL) and Open Database Connectivity (ODBC) as standards. These are but a few

examples of general IT standards that have had a real impact on the development and use of health care information systems.

In the sections that follow we provide an overview of the standards development process and introduce several key initiatives, some formal and some less so, that have led to the development of standards to facilitate interoperability among health care information systems. These standards will be reviewed in three main categories:

- Classification, vocabulary, and terminology standards
- Data interchange standards
- Health record content standards

We will conclude this chapter with a discussion of the impact of the recent HIPAA regulation on the adoption of health care information standards and a discussion of the latest developments in the move to establish the National Health Information Infrastructure.

Standards Development Process

When seeking to understand why so many different IT and health care information standards exist, it is helpful to look first at the basic standards development process that exists in the United States (and internationally) and the changes that have occurred in this process over the past decade. Four methods have been used to establish health care IT standards (Hammond & Cimino, 2001):

- *Ad hoc*. Standards are established by the ad hoc method when a group of interested people or organizations agrees on a certain specification without any formal adoption process. The Digital Imaging and Communications in Medicine (DICOM) standard for health care imaging came about in this way.
- *De facto*. A de facto standard arises when a vendor or other commercial enterprise controls such a large segment of the market that its product becomes the recognized norm. SQL and the Windows operating system are examples of de facto standards. Some individuals predict that XML will become a de facto standard for health care messaging.
- *Government mandate*. Standards are also established when the government mandates that the health care industry adopt them. Examples are the transaction and code sets mandated by the Health Insurance Portability and Accountability Act (HIPAA) regulations.
- *Consensus*. Consensus-based standards come about when volunteers from various interested groups come together to reach a formal agreement on specifications. The process is generally open and involves considering comment and feedback from

the industry. This method is employed by the American National Standards Institute (ANSI) accredited *standards development organizations* (SDOs). Most health care information standards are developed by this method, including Health Level 7 (HL7) standards and Accredited Standards Committee (ASC) X12N standards.

In a recent publication, Libicki, Schneider, Frelinger, and Slomovic (2000) outline a two-by-two matrix topology for IT standard-setting organizations. They classify the organizations that set IT standards by membership type (open to all or members only) and by whether the process employed is democratic or dependent on “a strong leader.” The organizations with the most formal standard-setting processes, such as the International Organization for Standardization (ISO), ANSI, and the ANSI-accredited SDOs, fall into the member-only, democratic classification. The relationships among the various standard-setting organizations can be confusing. Not only do many of the acronyms sound similar, but the organizations themselves, as voluntary, member-based organizations, can set their own missions and goals. Therefore, although there is a formally recognized relationship among ISO, ANSI, and the SDOs, there is also some overlap in activities. Table 9.1 outlines the relationships among these formal standard-setting organizations and for each one gives a brief overview of important facts and a current Web site.

All the ANSI-accredited SDOs must adhere to the guidelines established for accreditation; therefore they have similar standard-setting processes. According to ANSI, this process includes

- Consensus on a proposed standard by a group or “consensus body” that includes representatives from materially affected or interested parties;
- Broad-based public review and comment on draft standards;
- Consideration of and response to comments submitted by voting members of the relevant consensus body and by public review commenters;
- Incorporation of approved changes into a draft standard; and
- Right to appeal by any participant that believes that due process principles were not sufficiently respected during the standards development in accordance with the ANSI-accredited procedures of the standards developer [ANSI, 2004].

In the last decade the IT industry in general has experienced a movement away from the process of establishing standards via the SDOs. The Internet and World Wide Web standards, for example, were developed by groups with much less formal structures. The emergence of the Linux operating system has been cited as an example of a standard developed with minimal formal input. In fact in Libicki et al.’s typology (2000), the Linux development process would be furthest from the formal SDO process, as it was spearheaded by a strong leader with input from all.

**TABLE 9.1. ORGANIZATIONS RESPONSIBLE FOR
FORMAL STANDARDS DEVELOPMENT.**

Organizations	Facts
International Organization for Standardization (ISO), www.iso.org	• Members are national standards bodies from many different countries around the world. • ANSI is the U.S. national body member. • Oversees the flow of documentation and international approval of standards developed under the auspices of its member bodies.
American National Standards Institute (ANSI), www.ansi.org	• U.S. member of ISO • Accredits standards development organizations (SDOs) from a wide range of industries, including health care • Oversees the work of the SDOs, technical committees, subcommittees, and working groups • Does <i>not</i> develop standards itself, but accredits the organizations that develop standards • Publishes the 10,000+ American National Standards developed by accredited SDOs
Standards development organizations (SDOs)	• Must be accredited by ANSI • Develop standards in accordance with ANSI criteria
SDOs that develop health care–related standards discussed in this chapter: ASTM International (formerly American Society for Testing and Materials), www.astm.org Health Level 7 (HL7), www.hl7.org ANSI Accredited Standards Committee (ASC) X12, www.x12.org	• Can use the label “Approved American National Standard” • Currently, there are 270+ ANSI-accredited SDOs representing many industries, including health care

Classification, Vocabulary, and Terminology Standards

One of the most difficult problems in the exchange of health care information and building longitudinal electronic health records (EHRs) is coordinating the vast amount of health information that is generated in diverse locations for patients and populations. To date, no single vocabulary has emerged to meet all the information exchange needs of the health care sector. The most widely recognized coding and classification systems, ICD-9-CM, Current Procedural Terminology (CPT), and diagnosis related groups (DRGs), were discussed in Chapter One. Although these systems do not meet

the criteria for full clinical vocabularies, they are used to classify diagnoses and procedures and are the basis for information retrieval in health care information systems.

The National Committee on Vital and Health Statistics (NCVHS) has the responsibility, under a HIPAA mandate, to recommend uniform data standards for patient medical record information (PMRI). Although no single vocabulary has been recognized by NCVHS as “the” standard, in a November 2003 letter to Department of Health and Human Services secretary Tommy Thompson, NCVHS (2003) identified a core *set* of PMRI terminology standards:

- Systematized Nomenclature of Medicine—Clinical Terms (SNOMED CT)
- Logical Observation Identifiers Names and Codes (LOINC) laboratory subset
- Several federal drug terminologies, including RxNorm

In this section we will describe the PMRI terminologies recommended by NCVHS along with the National Library of Medicine’s Unified Medical Language, which has become the standard for bibliographical searches in health care, and has the potential for other uses as well.

Systematized Nomenclature of Medicine—Clinical Terms

Systematized Nomenclature of Medicine—Clinical Terms (SNOMED CT) is a comprehensive clinical terminology developed specifically to facilitate the electronic storage and retrieval of detailed clinical information. It is the result of collaboration between the College of American Pathologists (CAP) and the United Kingdom’s National Health Service (NHS). SNOMED CT merges the CAP’s SNOMED Reference Terminology, an older classification system used to group diseases, and the NHS’s Clinical Terms Version 3 (better known as Read Codes), an established clinical terminology used in Great Britain and elsewhere. As a result, SNOMED CT is based on decades of research.

The SNOMED CT core terminology “provides a common language that enables a consistent way of capturing, sharing, and aggregating health data across specialties and sites of care” (SNOMED International, 2003). SNOMED CT includes

- 344,000 concepts with unique meanings and formal logic-based definitions, organized as follows:
 - Finding (*swelling of arm*)
 - Disease (*pneumonia*)
 - Procedure (*biopsy of lung*)
 - Observable entity (*tumor stage*)
 - Body structure (*structure of thyroid*)
 - Organism (*DNA virus*)

Substance (*gastric acid*)
Pharmaceutical/biologic product (*tamoxifen*)
Specimen (*urine specimen*)
Physical object (*suture needle*)
Physical force (*friction*)
Events (*flash flood*)
Environments/geographical locations (*intensive care unit*)
Social context (*organ donor*)
Context-dependent categories (*no nausea*)
Staging and scales (*Nottingham ten-point ADL index assessment scale*)
Attribute (*controlled temperature*)
Qualifier value (*bilateral*)
Duplicate concept (*inactive concept*)

- 913,000 English language descriptions or synonyms for expressing clinical concepts
- Approximately 1.3 million semantic relationships to enable reliability and consistency of data retrieval

SNOMED CT is a comprehensive clinical terminology in its own right; however, it also maps to other classification systems that are currently in use, such as ICD-9-CM, ICD-10, laboratory LOINC, and others (SNOMED International, 2004).

Logical Observation Identifiers Names and Codes

The Logical Observation Identifiers Names and Codes (LOINC) system was developed to facilitate the electronic transmission of laboratory results to hospitals, physicians, third-party payers, and other users of laboratory data. Initiated in 1994 by the Regenstrief Institute at Indiana University, LOINC provides a standard set of universal names and codes for identifying individual laboratory and clinical results. These standard codes allow users to merge clinical results from disparate sources. LOINC is endorsed by the American Clinical Laboratory Association and CAP and contains about 32,000 observation terms, of which nearly 20,000 relate to laboratory testing. Each record in the LOINC database identifies a clinical observation and contains a formal six-part name and an identifying code with a check digit, synonyms, and other useful information. LOINC codes apply to all equivalent tests; they are not unique to tests from particular companies (LOINC, 2004).

Unified Medical Language System

The National Library of Medicine (NLM), an agency of the National Institutes of Health, began the Unified Medical Language System (UMLS) project in 1986, and it

is ongoing today. The purpose of the UMLS project is to “aid the development of systems that help health professionals and researchers retrieve and integrate electronic biomedical information from a variety of sources and make it easy for users to link disparate information systems, including computer-based patient records, bibliographic databases, factual databases and expert systems” (NLM, 2003, p. 1).

The UMLS has three basic components, called *knowledge sources*:

- UMLS Metathesaurus. Annual editions of the metathesaurus have been distributed by the NLM since 1990. The November 2003 edition included 975,354 concepts and 2.4 million concept names. All the common health information vocabularies, including SNOMED CT, ICD, and CPT, along with approximately 100 other vocabularies are incorporated into the metathesaurus. The metathesaurus project’s goal is to incorporate and map existing vocabularies into a single system.
- SPECIALIST Lexicon. The lexicon contains information for many terms, component words, and English language words that do not appear in the metathesaurus.
- UMLS Semantic Network. The semantic network contains information about the categories (such as “Disease or Syndrome” and “Virus”) to which metathesaurus concepts are assigned. The semantic network also outlines the relationships among the categories (for example, “Virus” causes “Disease or Syndrome”).

The UMLS products are widely used in NLM’s own applications, such as PubMed. They are available to other organizations free of charge, provided the users submit a license agreement (NLM, 2003).

RxNorm

RxNorm is an ongoing project within the UMLS. Its purpose is to define a nonproprietary drug vocabulary that “represents drugs at the level of granularity needed to support clinical practice” (NCVHS, 2003). Several experiments with RxNorm have been undertaken to date, but it is still considered a developing project. The NCVHS vocabulary recommendations include a request that additional funding be given to move the project along.

Data Interchange Standards

The ability to exchange and integrate data among health care applications is critical to the success of any overall health care information system, whether an organizational, regional, or national level of integration is desired. Much of the health care information standards development activity has been in the area of standards for data

interchange or integration. In this section we will look at a few of the standards that have been developed for this purpose. There are others, and new needs are continually being identified. However, the following groups of standards are recognized as important to the health care sector, and together they provide examples of both broad standards addressing all types of applications and specific standards addressing one type of application.

- Health Level Seven standards
- Digital Imaging and Communications in Medicine (DICOM)
- National Council for Prescription Drug Programs (NCPDP)
- ANSI X12N standards

Health Level Seven Standards

Health Level Seven (HL7) is an ANSI-accredited standards organization that was founded as an ad hoc group in 1987. HL7 was founded with a purpose of developing messaging standards to support the “exchange, management, and integration of data that support clinical patient care” (Marotta, 2000). Since its inception, HL7 has grown from a small group of 14 individuals to a large organization with nearly 2,000 health care provider, vendor, and consultant members. The HL7 messaging standard set of protocols has been widely adopted and used since Version 2.0 was released in the late 1980s. By the time the 2.4 Version was released, it had expanded to require 1,500 pages of detailed interfacing information (Kurtz, 2002). (Version 2.5 is the most recently approved version of the standard, but 3.0 is in active development at this time.) In 1998, the College of Healthcare Information Management Executives (CHIME) found the HL7 messaging standard to be the most widely used standard among health care providers (Marotta, 2000).

The name HL7 refers to the highest level in the OSI network reference model, the seventh layer. The HL7 set of messaging protocols is designed to deal with the network issues that occur at this level. They are

1. The data to be exchanged
2. The timing of the exchange
3. The communication of errors between applications

The first issue is addressed by compiling the data into a specific messaging format, which is defined by HL7’s encoding rules. The second issue is addressed through the use of HL7-defined *trigger events*, and the third is addressed by a set of protocols outlining a specific validation process (Van Hentenryck, 1998). Figure 9.1 presents an example of an HL7 encoded message. HL7 is not a static set of protocols. Significant changes to the standard are expected when Version 3.0 is released. Version 3.0 will gain even more functionality by incorporating XML (Marotta, 2000).

FIGURE 9.1. HL7 ENCODED MESSAGE.

This message is sent when a new patient arrives at the hospital. The patient's demographics are entered into the HIS (hospital information system) and then the information is communicated to all the other systems to avoid multiple entries of the patient's demographic information.

```
MSH|^~\&|EPIC|EPICADT|SMS|SMSADT|199912271408|CHARRIS|ADT^A04|1817457|D|2.3|
EVN|A04|199912271408|||CHARRIS
PID||0493575^^^2^ID 1|454721||DOE^JOHN^^^^|DOE^JOHN^^^^|19480203|M||B|254
E238ST^^EUCLID^OH^44123^USA|||(216)731-4359|||M|NON|400003403~1129086|999-|
NK1||CONROY^MARI^^^^|SPO|||(216)731-4359|EC|||||||||||||||||||||
PV1||O|168 ~219~C~PMA^^^^^^^^^^|277^ALLEN FADZL^BONNIE^^^^|2688684|
||2688684|||||199912271408|||||002376853
```

Source: Health Level Seven Canada, 2004.

In addition to messaging standards, the HL7 organization has published the following:

- Clinical Context Management (CCM) specifications (originally known as CCOW)
- Arden Syntax for Medical Logic Systems
- EHR functional model

CCM standards address the visual integration of disparate health care applications on the desktop. The purpose of these standards is to allow users to view results from different clinical systems on a single workstation. The goal is that the user will be able to view clinical results seamlessly, as if the systems were truly integrated. CCM does this by defining the content that must be shared by clinical applications during viewing, such as user password and the medical record number of the patient. The Arden Syntax can be used to encode medical logic, such as clinical reminders, alerts, interpretations, and diagnoses (Marotta, 2000). The most recent undertaking by HL7 is the development of an EHR functional model (discussed later in this chapter).

Digital Imaging and Communications in Medicine

The growth of digital diagnostic imaging (such as CAT scans and MRIs) gave rise to the need for a standard for the electronic transfer of these images between devices manufactured by different vendors. The American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) published the first standard, a precursor to the current Digital Imaging and

Communications in Medicine (DICOM) standard, in 1985. The stated purpose for the standard was to

- Promote communication of digital image information, regardless of device manufacturer
- Facilitate the development and expansion of picture archiving and communications systems (PACS) that can also interface with other systems of hospital information
- Allow the creation of diagnostic information data bases that can be interrogated by a wide variety of devices distributed geographically [NEMA, 2003, p. 5].

The current DICOM standard accomplishes these purposes by specifying (NEMA, 2003)

- A set of protocols for network communications
- The syntax and semantics of commands which can be used with these protocols
- A set of media storage services to be followed, including a file format and medical directory structure

National Council on Prescription Drug Programs

The mission of the National Council for Prescription Drug Programs (NCPDP) is to “create and promote data interchange standards for the pharmacy services sector of the health care industry, and to provide information and resources that educate the industry and support the diverse needs of its members” (NCPDP, 2004, p 5). To this end the NCPDP, an ANSI-accredited SDO, has developed a standard for the electronic submission of third-party drug claims. The standard addresses not only data format and content but also transmission and telecommunication protocols (Hammond & Cimino, 2001).

ASC X12N Standards

ANSI Accredited Standards Committee (ASC) X12 develops standards, in both X12 and XML formats, for the electronic exchange of business information. One ASC X12 subcommittee, X12N, has been specifically designated to deal with electronic data interchange (EDI) standards in the insurance industry, and this subcommittee has a special health care task group, known as TG2. According to the X12/TG2 Web site: “the purpose of the Health Care Task group shall be the development and maintenance of data standards (both national and international) which shall support the exchange of business information for health care administration. Health care data

includes, but is not limited to, such business functions as eligibility, referrals and authorizations, claims, claim status, payment and remittance advice, and provider directories” (Accredited Standards Committee X12, 2004).

Health Record Content Standards

In this section we will look at two set of standards currently being developed. The first is the HL7 EHR Functional Model and the second is the ASTM Healthcare Informatics subcommittee’s Continuity of Care Record (CCR) standard. Although these standards are being developed for different purposes, both address the content of the patient’s electronic health record.

HL7 EHR Functional Model

The need for recognized functional standards for the EHR is not new. Beginning with the landmark Institute of Medicine (IOM) study of patient records in 1991, multiple efforts have been made to address this issue. However, in the very recent past, efforts to develop an EHR functional standard have intensified. In July 2003, the IOM (2003a) released a letter report calling for a functional model of the EHR. By August 2003, HL7 had released a draft version of the EHR Functional Model and Standard. Not only the IOM and HL7 but also a variety of professional organizations have been involved in this process, including the following, who serve as members of the EHR Collaborative (2004), a vehicle for presenting and discussing the proposed EHR Functional Model:

- American Health Information Management Association (AHIMA)
- American Medical Association (AMA)
- American Nurses Association (ANA)
- American Medical Informatics Association (AMIA)
- College of Healthcare Information Management Executives (CHIME)
- eHealth Initiative (eHI)
- Healthcare Information and Management Systems Society (HIMSS)
- National Alliance for Health Information Technology (NAHIT)

A second draft of the EHR Functional Model was adopted in 2004, after input from many sectors of the health care industry under the leadership of HL7. The EHR Functional Model is an application-neutral model that focuses on defining the contents of an EHR. The model is divided into three components, *direct care*, *supportive*, and *information infrastructure* (Wise and Mon, 2004). Figure 9.2 shows excerpts from each of these sections.

FIGURE 9.2. HL7 EHR FUNCTIONAL MODEL OUTLINE.

Direct Care	DC1.0	Care Management
	DC2.0	Clinical Decision Support
	DC3.0	Operations Management and Communication
Supportive	S1.0	Clinical Support
	S2.0	Measurement, Analysis, Research, Reporting
	S3.0	Administrative and Financial
Information Infrastructure	I 1.0	EHR Security
	I 2.0	EHR Information and Records Management
	I 3.0	Unique identity, registry, and directory services
	I 4.0	Support for Health Informatics & Terminology Standards
	I 5.0	Interoperability
	I 6.0	Manage business rules
	I 7.0	Workflow

Source: Wise & Mon, 2004, slide 16.

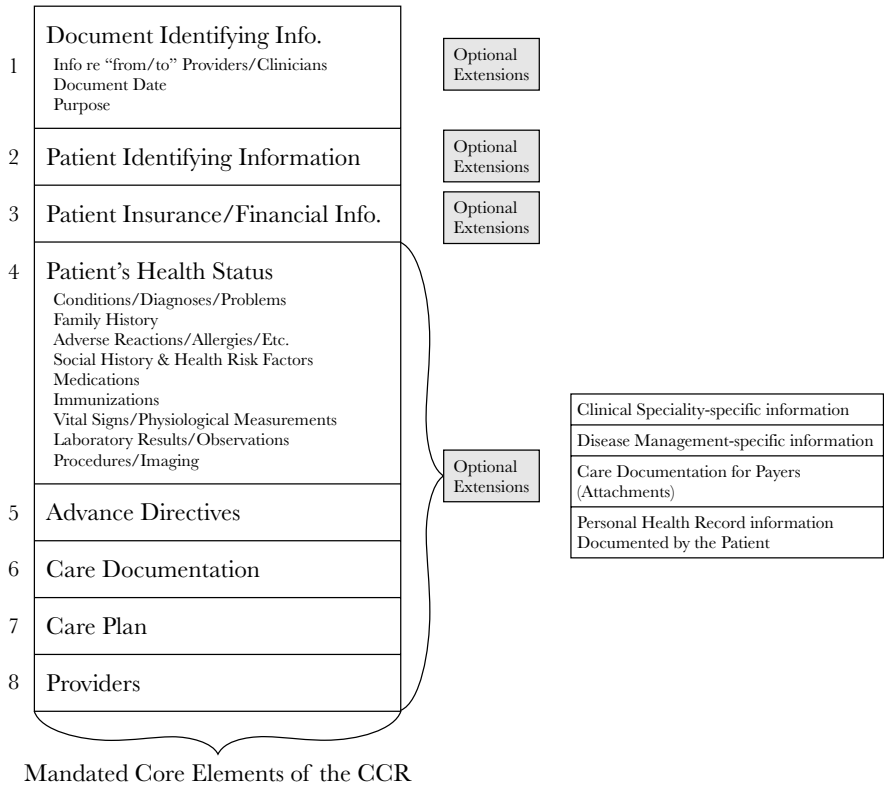
Continuity of Care Record Standard

The Continuity of Care Record (CCR) standard is being developed under the auspices of the ASTM Healthcare Informatics subcommittee, with participation from the Health Care Information and Management Systems Society (HIMSS), the American Academy of Family Physicians (AAFP), and the American Academy of Pediatrics (AAP). The CCR is intended to provide the core data set of the most relevant and timely facts about a patient's health care. As currently envisioned, the CCR will be prepared by the provider at the end of a health care encounter in order to provide a summary of the patient's health status that can be used by any other providers the patient subsequently sees. The CCR will be completed when a patient is being referred or transferred to another health care provider. It may be completed by a physician, nurse, or other ancillary health care provider, such as a social worker or physical therapist. It will be an XML standard document, capable of being displayed in a variety of formats, including word processor formats, PDF formats, and Web

formats (MRI, 2004a). Figure 9.3 shows the mandated core and optional extensions of Version 3 of the conceptual model of the CCR. In Version 3 of the CCR model, the mandated core includes eight elements:

- 1. Document identifying information (Header): contains information about the referring source and receiving source, the date, and the reason for the referral or transfer
- 2. Patient identifying information
- 3. Patient insurance and financial information
- 4. Patient’s health status
- 5. Advance directives
- 6. Care documentation
- 7. Care plan
- 8. Providers

FIGURE 9.3. CONCEPTUAL MODEL OF THE CCR.



Source: Medical Records Institute, 2004a.

Impact of HIPAA on Health Care Information Standards

In August 2000, the Department of Health and Human Services published the final rule outlining the standards to be adopted by health care organizations for electronic transactions, and announced the *designated standard maintenance organizations* (DSMOs). Modifications to this final rule were subsequently published in 2002. In publishing this rule the federal government mandated that health care organizations adopt certain standards for electronic transactions and identified the standards organizations that would oversee the adoption of standards for HIPAA compliance.

The majority of the HIPAA transaction standards were taken from ASC X12N standards. Specifically, the transaction standards cited in the HIPAA regulations (42 C.F.R. Part 162, 2003) are

- Health Care Claims or equivalent encounter information (X12N 837)
- Eligibility for a Health Plan (X12N 270/271)
- Referral Certification and Authorization (X12N 278, or NCPDP for retail pharmacy)
- Health Care Claim Status (X12N 276/277)
- Enrollment and Disenrollment in a Health Plan (X12N 834)
- Health Care Payment and Remittance Advice (X12N 835)
- Health Plan Premium Payments (X12N 820)
- Coordination of Benefits (X12N 837, or NCPDP for retail pharmacy)

In addition to these transaction standards, several standard code sets were also established for use in electronic transactions. These code sets (a topic discussed in earlier chapters) include

- International Classification of Diseases, ninth edition, clinical modification (ICD-9-CM)
- Code on Dental Procedures and Nomenclature (CDT)
- Healthcare Common Procedural Coding System (HCPCS)
- Current Procedural Terminology, fourth edition (CPT-4).

The role of the DSMOs, as outlined in the regulation, is to take responsibility for the development, maintenance, and modification of relevant electronic data interchange standards. Currently, the following organizations are recognized by the federal government as DSMOs. All except the Dental Content Committee have been discussed in this text. All are significant players in the establishment of health care information standards.

- Accredited Standards Committee X12 (ANSI ASC X12)
- Dental Content Committee of the American Dental Association (ADA DCC)
- Health Level Seven (HL7)
- National Council for Prescription Drug Programs (NCPDP)
- National Uniform Billing Committee (NUBC)
- National Uniform Claim Committee (NUCC)

National Healthcare Information Infrastructure

In 2001, the National Committee on Vital and Health Statistics (NCVHS) published a report, *Information for Health: A Strategy for Building the National Health Information Infrastructure*, that outlines the “vision and process for building the NHII.” We have observed some confusion about what the National Healthcare Information Infrastructure (NHII) is and what it is not. First of all, the NHII is not simply a set of nationally adopted health information standards, although standards are certainly necessary for a successful NHII. The vision for the NHII goes well beyond standards and includes actually building this infrastructure. Second, the NHII is not a governmental agency, program, or regulation. The role of the government in the development and building of the NHII is one of facilitator and coordinator. The NCVHS serves as the public advisory committee for the NHII to the secretary of Health and Human Services, but many other agencies are also involved in promoting related activities. There is a definite role for government in the processes of adopting standards, incorporating privacy and security, and funding research and other projects. Third, the NHII is not a centralized database of medical records. EHRs will certainly be an important part of the NHII, but it does not include a national, central database of EHR information.

What then is the NHII? The NHII (when realized) will be a “comprehensive knowledge-based network of interoperable systems of clinical, public health, and personal health information that would improve decision-making by making health information available when and where it is needed” (NCVHS, 2001, p. 1). The NHII will include technologies, standards, applications, systems, values, and laws in order to improve patient safety and health care quality. Other stated benefits of the NHII would be bioterrorism detection, better informed and empowered health care consumers, and a better overall understanding of true health care costs. The NHII has three overlapping dimensions (HHS, 2004):

1. Personal health: includes a personal health record created and controlled by an individual or family member.

2. Health care delivery: includes clinical information from the providers of care, including decision-support programs and practice guidelines; providers would maintain control of their own patients' health records.
3. Public health: this includes such things as vital statistics, population health information, and disease registries to improve the clinical management of population health.

Many challenges must be met and barriers surmounted before the NHII can be fully realized. Health care delivery in the United States is a large, complex, and fragmented activity, and information technology to support health care is expensive. Several specific barriers to the realization of the NHII in this environment have been cited (HHS, 2004):

- Lack of standards for system interoperability
- Lack of incentives for establishing electronic systems at the point of care
- Insufficient funding for related projects
- Privacy and security concerns

Another barrier is the uncertainty regarding the technical infrastructure for linking patient records across multiple provider organizations. Many argue that the NHII will be constructed by linking *local healthcare information infrastructures* (LHIIs): for example, linking an LHII in Boston with one in Indianapolis. There are a surprising number of LHIIs in development—over 100 as of 2004 (see eHealth Initiative, 2004, for an overview and inventory of LHII efforts).

There is much to be accomplished before the NHII is a reality. However, it has become an important joint governmental and private sector initiative. The NCVHS report (2001) outlines an aggressive three-stage, ten-year plan for achieving the vision of the NHII. The first stage (within two years) was to identify leadership in governmental agencies to “flesh out the vision of implementation and policy.” This stage was realized in April 2004, when President Bush announced the creation of the Office of the National Coordinator for Health Information Technology, which will oversee national NHII efforts. The second stage (within five years) is to build collaboration among stakeholders, and the third stage (within ten years) “involves carrying out the plan in all relevant public and private sectors” (HHS, 2004).

Summary

In this chapter we reviewed the processes by which health care information standards are developed, and looked at some of the more common standards that exist today, including standards in three main categories: classification, vocabulary, and terminology standards; data interchange standards; and health record content standards.

Multiple standard-setting organizations and health care professional organizations play a role in standards development. Standards can be developed through a formal process or by less formal mechanisms, including de facto designation.

The standards discussed in this chapter and other general IT standards enable health care information systems to be interoperable and portable and to exchange data. Without such standards the EMR system and other health care information systems would have limited functionality.

The future of health care information systems is unknown; however, it is clear that the goal of having functional EHRs will not be realized until national standards are adopted. The government, as well as the private sector, plays a role in the development of national standards. HIPAA, for example, has had an impact on the development of health care information standards through designating required transaction and code sets to be used, and the recent National Healthcare Information Infrastructure, spearheaded by the NCVHS, is receiving a lot of national attention.

Chapter Nine: Learning Activities

1. Standards development is a dynamic process. Select one or more of the standards listed in this chapter and conduct an Internet search for information on that standard. Has the standard changed? What are the current issues surrounding the standard?
2. Visit a hospital IT department, and speak with a clinical analyst or other person who works with clinical applications. Investigate the standards that the hospital's applications use. Discuss any issues surrounding these standards.
3. Interview the CIO of a health care organization. Find out his or her views on the current state of health care IT standards or on the need for standards as the United States moves toward broader adoption of EMR systems.



CHAPTER TEN

SECURITY OF HEALTH CARE INFORMATION SYSTEMS

By now it should be clear that much of the information in today's health care organizations is transmitted, maintained, and stored electronically. Electronic medical record (EMR) systems are becoming more common, but, as we have seen, even primarily paper-based health care information systems contain data and information that have been created and transmitted electronically.

In this chapter we define *security*, examine the need for establishing an organization-wide security program, and discuss a variety of security-related topics. We also look at the various existing threats to health care information. In addition, we present an outline of the components of the HIPAA security regulations. Although security concerns certainly predate the implementation of the HIPAA Security Rule, the standards in this rule provide an excellent and comprehensive outline of the components necessary for securing health information and, to some extent, provide a framework for establishing a viable health care information security program. The chapter will then continue with a look at the following specific topics, including examples of actual practices and procedures:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

The chapter concludes with a discussion of the special security issues associated with increased use of wireless networks and related devices in health care organizations.

Introduction to a Health Care Organization Security Program

Health care organizations must protect their information systems from a range of potential threats. Among these threats are viruses, fire in the computer room, untested software, and employee theft of clinical and administrative data. Threats may also involve intentional or unintentional damage to hardware, software, or data or misuse of the organization's hardware, software, or data. The realization of any of these threats can cause significant damage to the organization. Resorting to manual operations if the computers are down for days can lead to organizational chaos. Theft of organizational data can lead to litigation by the individuals harmed by the disclosure of the data. Viruses can corrupt databases, corruption from which there may be no recovery. Health care organizations must have programs in place to combat security breaches.

A health care organization's security program involves identifying potential threats and implementing processes to remove the threats or mitigate their ability to cause damage. For example, the use of antivirus software is designed to reduce the threat from viruses; the installation of fire protection systems in computer rooms is intended to reduce the damage that might be caused by a fire.

It is important to understand how patient privacy is related to security. The intentional or unintentional release of patient-identifiable information constitutes a misuse of the organization's information systems. Security in a health care organization should be designed, however, to protect not only patient-specific information but also the organization's IT assets—such as the networks, hardware, software, and applications that make up the organization's health care information systems—from potential threats, both threats that come from human beings and those from natural and environmental causes.

The primary challenge of developing an effective security program in a health care organization is balancing the need for security with the cost of security. An organization does not know how to calculate the likelihood that a hacker will cause serious damage or a backhoe will cut through network cables under the street. The organization may not fully understand the consequences of being without its network for four hours or four days. Hence, it may not be sure how much to spend to remove or reduce the risk. This dilemma is similar to the one posed when individuals consider obtaining long-term care insurance. None of us know whether we will or will not need this insurance, how long we might live in a long-term care facility, or the acuity of the care we may need. How much insurance should we buy?

One aspect of this trade-off is maintaining a satisfactory balance between health care information system security and health care data and information availability. As we saw in Chapter One, the major purpose of maintaining health information and health records is to facilitate high-quality care for patients. On the one hand, if an organization's

security measures are so stringent that they prevent appropriate access to the health information needed to care for patients, this important purpose is undermined. On the other hand, if the organization allows unrestricted access to all patient-identifiable information to all its employees, the patients' rights to privacy and confidentiality would certainly be violated and the organization's IT assets would be at considerable risk.

As health care organizations develop their security programs they should be sure to seek input from a wide range of health care providers and other system users as well as legal counsel and technical experts. The balance between access and security should be reasonable—protecting patients' rights while allowing appropriate access.

Threats to Health Care Information

What are the threats to health care information systems? In general, threats to health care information systems will fall into one of these three categories:

- Human threats, which can result from intentional or unintentional human tampering
- Natural and environmental threats, such as floods, fires, and power outages
- Technology malfunctions, such as a drive that fails and has no backup

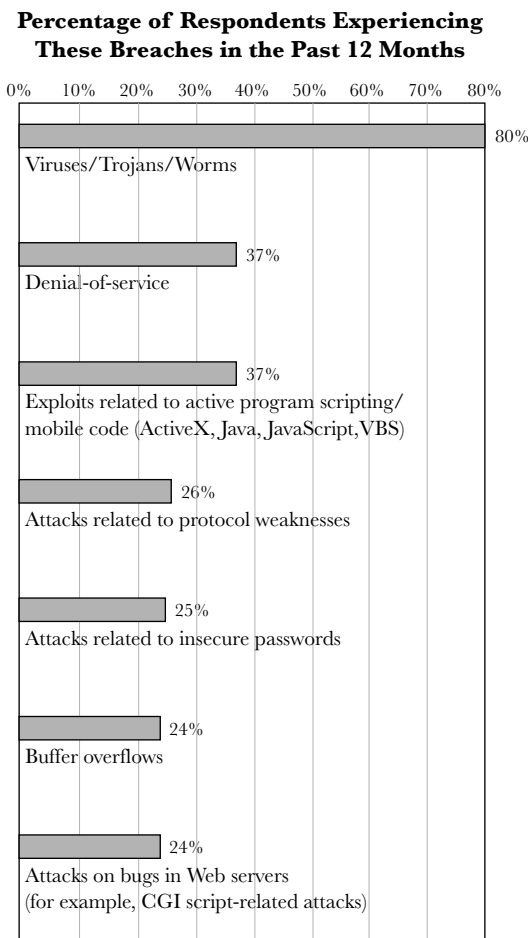
Within these categories are multiple potential threats. Threats to health care information systems from human beings can be *intentional* or *unintentional*. They can be *internal*, caused by employees, or *external*, caused by individuals outside the organization. Intentional threats include theft, intentional alteration of data, and intentional destruction of data. The culprit could be a disgruntled employee, a computer hacker, or a prankster. In a Florida case several years ago, for example, the daughter of a hospital employee accessed confidential information through an unattended computer workstation in the facility's emergency room. She wrote down names and addresses of recent patients and then called to tell them that they had tested positive for HIV. Several of the recipients of these prank calls became extremely distraught (Associated Press, 1995a, 1995b; Lee, in press).

Computer viruses are among the most common and virulent forms of intentional computer tampering. They pose a serious threat to computerized patient data and health care applications. According to a 2001 survey conducted by *Information Security* magazine (Briney, 2001), 89 percent of the organizations surveyed experienced a breach in security due to a virus, Trojan horse, or worm attack. Forty-eight percent suffered from attacks on known flaws, or *bugs*, in their Web servers. Figure 10.1 summarizes the causes of external breaches reported by a similar survey conducted in mid-2000. Virus attacks are costly to organizations. Many of the costs are *soft* costs, such as downtime and loss of productivity. In May 2000, the infamous worm called

LoveLetter swept across the world, causing somewhere between \$700 million and \$15 billion in damage and downtime (Briney, 2000). (See the section on virus checking later in this chapter for more information on viruses.)

Some of the causes of unintentional damage to health care information systems are lack of training in proper use of the system or human error. When users share

FIGURE 10.1. OUTSIDER BREACHES.



¹ “Outsider” refers to everyone not included in the description for “insider” in the opposite chart.

Note: Outsider refers to everyone not included in the description of insider in Figure 10.2.

Source: Briney, 2000.

passwords or download information from a nonsecure Internet site for example, they create the potential for a breach in security.

According to the 2001 *Information Security* magazine survey, *internal* breaches of security are far more common than *external* breaches. The most common forms of internal breaches of security across all industries are the installation or use of unauthorized software, use of the organization's computing resources for illegal or illicit communications or activities (porn surfing, e-mail harassment, and so forth), and the use of the organization's computing resources for personal profit (Briney, 2000). Figure 10.2 summarizes the causes of insider breaches found by the 2000 survey.

Computer hardware used in health care information systems must also be protected from loss. Safeware, The Insurance Agency, Inc. published the projected losses for the personal computers and notebook computers it insured during 2002 (Table 10.1). The major cause of computer loss for this insured population was accident, and the next greatest cause was theft. Natural and environmental causes, such as power surges, lightning, and water damage, were also significant factors in hardware loss.

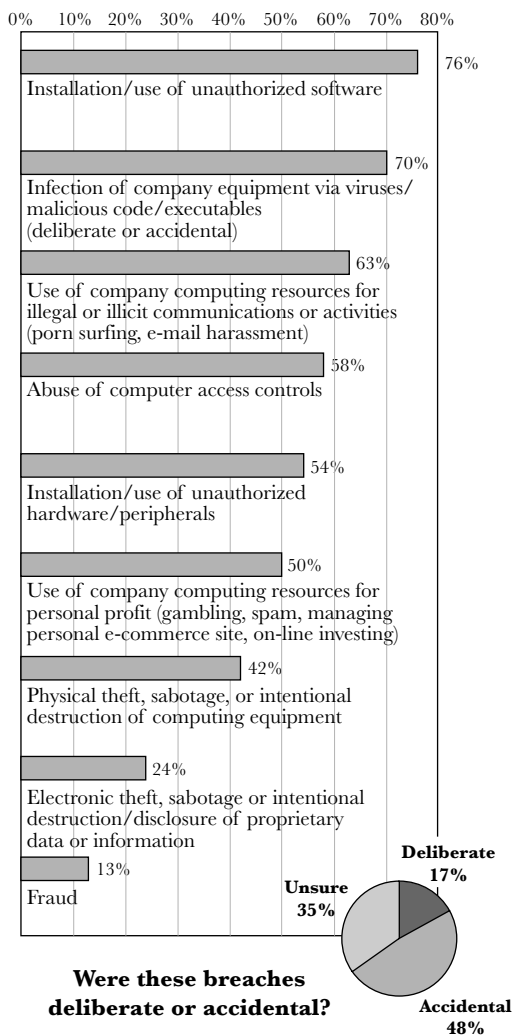
Electronic health care information is vulnerable to internal and external threats. Whether intentional or unintentional, these threats pose serious security risks. To minimize the risk and protect patients' sensitive health care information, well-established and well-implemented administrative, physical, and technical security safeguards are essential for any health care organization, regardless of size.

TABLE 10.1. AN INSURER'S PERSONAL LOSS CLAIMS FOR HARDWARE IN 2002.

Cause of Loss	2002 Number (000s)	% of Total	2001 Number (000s)	% of Total	Increase or Decrease Compared to Prior Year
Accidents	2,977	72%	1,415	59%	110
Theft	620	15	606	25	2
Power surge	37	1	89	4	-58
Lightning	38	1	51	2	-25
Transit	1	0	33	1	-97
Water or flood	379	9	169	7	124
Other	64	2	37	2	73
TOTAL	4,116	100%	2,400	100%	72

Note: Losses projected from actual claims reported by Safeware's national client base.

Source: Safeware, 2003.

FIGURE 10.2. INSIDER BREACHES.**Percentage of Respondents Experiencing These Breaches in the Past 12 Months**

Note: Insider refers to full-time or part-time employees, contract workers, consultants, company partners, and suppliers.

Source: Briney, 2000.

The security standards established by the Department of Health and Human Services under the terms of the Health Insurance Portability and Accountability Act (HIPAA) provide an excellent framework for developing an overall security plan and program for a health care institution. The regulations are designed to be flexible and scalable and are not reliant on specific technologies for implementation, making it possible for health care organizations of all sizes to be compliant.

Overview of HIPAA Security Standards: Final Rule

The final rule on the HIPAA security standards, known generally as the Security Rule, was published in the Federal Register on February 20, 2003 (68 Fed. Reg. 34, 8333–8381). (In Chapter Three we looked at the various components of the far-reaching HIPAA legislation. In this section we discuss the security component in greater detail. You may wish to refer back to Chapter Three for a description of how the Security Rule fits into the overall Act.) Covered entities (CEs) have two years to comply with the rules. Most CEs will be required to comply with the HIPAA Security Rule no later than April 2005. The HIPAA Security Rule is closely connected to the HIPAA Privacy Rule (as discussed in Chapter Three). However, whereas the Privacy Rule governs all protected health information (PHI), the Security Rule governs only *ePHI*. *ePHI* is defined as the protected health information maintained or transmitted in electronic form. The Security Rule does not distinguish between electronic forms of information or between transmission mechanisms. *ePHI* may be stored in any type of electronic media, such as magnetic tapes and disks, optical disks, servers, and personal computers. Transmission may take place over the Internet, on local area networks (LANs), or by disks, for example.

The HIPAA Security Rule was first published in draft form, in August 1998. At that time one of the complaints was that the standards were too prescriptive and not flexible enough. As a result the standards in the final rule are defined in general terms, focusing on what should be done rather than on how it should be done. According to the Centers for Medicare and Medicaid Services (CMS, 2004), the final rule specifies “a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications” (see also Quinsley, 2004; American Health Information Management Association, 2003a; Gue, 2003).

There are few key terms to be defined before we examine the content of the HIPAA Security Rule. What is a covered entity? What is the difference between a required implementation specification and an addressable one?

The HIPAA standards govern *covered entities* (CEs), which are defined as

- A health plan.
- A health care clearinghouse.
- A health care provider who transmits protected health information in electronic form. This includes practically every type of health care organization imaginable, including hospitals, clinics, physician's offices, nursing homes, and so forth.

The specifications contained in the Security Rule are designated as either *required* or *addressable*. A required specification must be implemented by a CE for that organization to be in compliance. However, the CE is in compliance of an addressable specification if it does any one of the following:

- Implements the specification as stated.
- Implements an alternative security measure to accomplish the purposes of the standard or specification.
- Chooses not to implement anything, provided it can demonstrate that the standard or specification is not reasonable and appropriate and that the standard can still be met. Because the Security Rule is designed to be technology neutral, this flexibility was granted for organizations that employ nonstandard technologies or have legitimate reasons not to need the stated specification (AHIMA, 2003a; Gue, 2003).

The standards contained in the HIPAA Security Rule are divided into five sections, or categories, the specifics of which we will outline here. You will notice overlap among the sections. For example, contingency plans are covered under both administrative and physical safeguards, and access controls are addressed in several standards and specifications. In subsequent sections of this chapter we will look at some actual practices that might be employed by health care organizations in each of the first four categories. As you read through this outline, consider how it would work as a framework or model for a health care organization's security program.

Outline of HIPAA Security Standards: Final Rule

The Administrative Safeguards section contains nine standards:

1. *Security management functions*. This standard requires the CE to implement policies and procedures to prevent, detect, contain, and correct security violations. There are four implementation specifications for this standard:

- *Risk analysis* (required). The CE must conduct an accurate and thorough assessment of the potential risks to and vulnerabilities of the confidentiality, integrity, and availability of ePHI.
 - *Risk management* (required). The CE must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
 - *Sanction policy* (required). The CE must apply appropriate sanctions against workforce members who fail to comply with the CE's security policies and procedures.
 - *Information system activity review* (required). The CE must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
2. *Assigned security responsibility*. This standard does not have any implementation specifications. It requires the CE to identify the individual responsible for overseeing development of the organization's security policies and procedures.
3. *Workforce security*. This standard requires the CE to implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI and to prevent those workforce members who do not have access from obtaining access. There are three implementation specifications for this standard:
- *Authorization and/or supervision* (addressable). The CE must have a process for ensuring that the workforce working with ePHI has adequate authorization and/or supervision.
 - *Workforce clearance procedure* (addressable). There must be a process to determine what access is appropriate for each workforce member.
 - *Termination procedures* (addressable). There must be a process for terminating access to ePHI when a workforce member is no longer employed or his or her responsibilities change.
4. *Information access management*. This standard requires the CE to implement policies and procedures for authorizing access to ePHI. There are three implementation specifications within this standard. The first (not shown here) applies to health care clearinghouses, and the other two apply to health care organizations:
- *Access authorization* (addressable). The CE must have a process for granting access to ePHI through a workstation, transaction, program, or other process.
 - *Access establishment and modification* (addressable). The CE must have a process (based on the access authorization) to establish, document, review, and modify a user's right to access to a workstation, transaction, program, or process.

5. *Security awareness and training*. This standard requires the CE to implement awareness and training programs for all members of its workforce. This training should include periodic security reminders and address protection from malicious software, log-in monitoring, and password management. (These items to be addressed in training are all listed as addressable implementation specifications.)
6. *Security incident reporting*. This standard requires the CE to implement policies and procedures to address security incidents.
7. *Contingency plan*. This standard has five implementation specifications:
 - *Data backup plan* (required).
 - *Disaster recovery plan* (required).
 - *Emergency mode operation plan* (required).
 - *Testing and revision procedures* (addressable). The CE should periodically test and modify all contingency plans.
 - *Applications and data criticality analysis* (addressable). The CE should assess the relative criticality of specific applications and data in support of its contingency plan.
8. *Evaluation*. This standard requires the CE to periodically perform technical and nontechnical evaluations in response to changes that may affect the security of ePHI.
9. *Business associate contracts and other arrangements*. This standard outlines the conditions under which a CE must have a formal agreement with business associates to exchange ePHI.

The Physical Safeguards section contains four standards:

1. *Facility access controls*. This standard requires the CE to implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed to authorized users. There are four implementation specifications with this standard:
 - *Contingency operations* (addressable). The CE should have a process for allowing facility access to support the restoration of lost data under the disaster recovery plan and emergency mode operation plan.
 - *Facility security plan* (addressable). The CE must have a process to safeguard the facility and its equipment from unauthorized access, tampering, and theft.
 - *Access control and validation* (addressable). The CE should have a process to control and validate access to facilities based on users' roles or functions.
 - *Maintenance records* (addressable). The CE should have a process to document repairs and modifications to the physical components of a facility as they relate to security.

2. *Workstation use.* This standard requires the CE to implement policies and procedures that specify the proper functions to be performed and the manner in which those functions are to be performed on a specific workstation or class of workstation that can be used to access ePHI, and that specify the physical attributes of the surroundings of such workstations.
3. *Workstation security.* This standard requires the CE to implement physical safeguards for all workstations that are used to access ePHI and to restrict access to authorized users.
4. *Device and media controls.* This standard requires the CE to implement policies and procedures for the movement of hardware and electronic media that contain ePHI into and out of a facility and within a facility. There are four implementation specifications with this standard:
 - *Disposal* (required). The CE must have a process for the final disposition of ePHI and of the hardware and electronic media on which it is stored.
 - *Media re-use* (required). The CE must have a process for removal of ePHI from electronic media before the media can be re-used.
 - *Accountability* (addressable). The CE must maintain a record of movements of hardware and electronic media and any person responsible for these items.
 - *Data backup and storage* (addressable). The CE must create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

The Technical Safeguards section has five standards:

1. *Access control.* This standard requires the CE to implement technical policies and procedures for electronic information systems that maintain ePHI in order to allow access only to those persons or software programs that have been granted access rights as specified in the administrative safeguards. There are four implementation specifications with this standard:
 - *Unique user identification* (required). The CE must assign a unique name or number for identifying and tracking each user's identity.
 - *Emergency access procedure* (required). The CE must establish procedures for obtaining necessary ePHI in an emergency.
 - *Automatic logoff* (addressable). The CE must implement electronic processes that terminate an electronic session after a predetermined time of inactivity.
 - *Encryption and decryption* (addressable). The CE should implement a mechanism to encrypt and decrypt ePHI as needed.
2. *Audit controls.* This standard requires the CE to implement hardware, software, and procedures that record and examine activity in the information systems that contain ePHI.

3. *Integrity*. This standard requires the CE to implement policies and procedures to protect ePHI from improper alteration or destruction.
4. *Person or entity authentication*. This standard requires the CE to implement procedures to verify that a person or entity seeking access to ePHI is in fact the person or entity claimed.
5. *Transmission security*. This standard requires the CE to implement technical measures to guard against unauthorized access to ePHI being transmitted across a network. There are two implementation specifications with this standard:
 - *Integrity controls* (addressable). The CE must implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection.
 - *Encryption* (addressable). The CE should encrypt ePHI whenever it is deemed appropriate.

The Policies, Procedures, and Documentation section has two standards:

1. *Policies and procedures*. This standard requires the CE to establish and implement policies and procedures to comply with the standards, implementation specifications, and other requirements.
2. *Documentation*. This standard requires the CE to maintain the policies and procedures implemented to comply with the security rule in written form. There are three implementation specifications:
 - *Time limit* (required). The CE must retain the documentation for six years from the date of its creation or the date when it was last in effect, whichever is later.
 - *Availability* (required). The CE must make the documentation available to those persons responsible for implementing the policies and procedures.
 - *Updates* (required). The CE must review the documentation periodically and update it as needed.

This section has provided an outline of the key components of the HIPAA security standards (68 Fed. Reg. 34, 8333–8381, Feb. 20, 2003). In the next sections we will examine some of the practices that can be employed to address the regulations and ensure that an organization has an effective security program.

Administrative Safeguards

As you have seen from the HIPAA standards outline, administrative safeguards cover a wide range of organization activities. We do not attempt in this section to give a comprehensive, detailed view of all possible administrative safeguards but rather to

present a few practices that can be used as part of a total administrative effort to improve the health care organization's information security program. We will discuss the following topics (Lee, in press):

- Risk analysis and management
- Chief security officer
- System security evaluation

Risk Analysis and Management

One of the key components of applying administrative safeguards to protect the organization's health care information is risk analysis. It is impossible to establish an effective risk management program if the organization is not aware of the risks or threats that exist. Risk analysis is relatively new to health care. Few organizations had implemented formal security risk assessment prior to the publication of the HIPAA rules. This in no way minimizes its importance. However, health care has had to look to other industries for examples of risk assessment processes (Walsh, 2003).

Steve Weil (2004), in a recent article posted to HIPAAAdvisory.com, defines risk as the "likelihood that a specific threat will exploit a certain vulnerability, and the resulting impact of that event." He introduces a risk analysis process with eight parts, or steps:

1. *Boundary definition.* During the boundary definition step the organization should develop a detailed inventory of all health information and information systems. This review can be conducted using interviews, inspections, questionnaires, or other means. The important thing in this step is to identify all the patient-specific health information, health care information systems (both internal and external), and users of the information and systems.
2. *Threat identification.* Identifying threats will result in a list of all potential threats to the organization's health care information systems. The three general types of threats that should be considered are
 - a. Natural, such as floods and fires
 - b. Human, which can be intentional or unintentional
 - c. Environmental, such as power outages
3. *Vulnerability identification.* In this step the organization identifies all the specific vulnerabilities that exist in its own health care information systems. Generally, vulnerabilities take the form of flaws or weaknesses in system procedures or design. Software packages are available to assist with identifying vulnerabilities, but the organization may also need to conduct interviews, surveys, and the like. Some organizations may employ external consultants to help them identify the vulnerabilities in their systems.

4. *Security control analysis.* The organization also needs to conduct a thorough analysis of the security controls that are currently in place. These controls include both preventive controls, such as access controls and authentication procedures, and controls designed to detect actual or potential breaches, such as audit trails and alarms.
5. *Risk likelihood determination.* This step in the process involves assigning a *risk rating* to each area of the health care information system. There are a variety of rating systems that may be employed. Weil recommends using a fairly straightforward high-risk, medium-risk, and low-risk system of rating.
6. *Impact analysis.* This is the step in which the organization determines what the actual impact of specific security breaches would be. A breach may affect confidentiality, integrity, or availability. Impact too can be rated as high, medium, or low.
7. *Risk determination.* The information gathered up to this point in the risk analysis process is now brought together in order to determine the actual level of risk to specific information and specific information systems. The risk determination is based on
 - a. The likelihood that a certain threat will attempt to exploit a specific vulnerability (high, medium, or low)
 - b. The level of impact should the threat successfully exploit the vulnerability (high, medium, or low)
 - c. The adequacy of planned or existing security controls (high, medium, or low)Each specific system or type of information can be assessed for each of these three factors, and then these assessments can be combined to produce an overall risk rating of high—needing immediate attention, medium—needing attention soon, or low—existing controls are acceptable.
8. *Security control recommendations.* The final step of the process is to compile a summary report on the findings of the analysis and recommendations for improving security controls.

The risk analysis should lead to the development of policies and procedures outlining risk management procedures and sanctions or consequences for employees and other individuals who do not follow the established procedures. All health care organizations should have a formal security risk management program in place. In general, this program is administered by the organization's security officer.

Chief Security Officer

Each health care organization must have a single individual who is responsible for overseeing the information security program. Generally, this individual is identified as the organization's *chief security officer*. The chief security officer may report to the chief

information officer (CIO) or to another administrator in the health care organization. The role of security officer may be 100 percent of an individual's job responsibilities or only a fraction, depending on the size of the organization and the scope of its health care information systems. Regardless of the actual reporting structure, it is essential that the chief security officer be given the authority to effectively manage the security program, apply sanctions, and influence employees. As Tom Walsh (2003, p. 15) stated in identifying the importance of the security officer, "influence can leverage the right people to get the job done."

System Security Evaluation

Chief security officers must periodically evaluate their organization's health care information systems and networks for proper technical controls and processes. Clearly, an established set of health information technical standards for security would facilitate this evaluation process. Unfortunately, there are currently no widely adopted *technical* security standards designed for health care information systems (and recall from our earlier discussion that the HIPAA standards are technology neutral). Efforts have been made, however, toward developing recognized, global information technology (IT) security standards. One source of such standards is the Department of Defense publication *Trusted Computer System Evaluation Criteria* (TCSEC). It is sometimes referred to as the Orange Book, due to the color of its cover. The Orange Book provides a rating system broken into four categories, Decision A through Decision D. Decision D is the lowest-level security rating, indicating a system with no inherent security features. Decision A is the highest level, the rating that is to be achieved by U.S. military computers. Each of the four categories is further divided into numbered subclasses, with 1 representing the highest-level security within any decision category. A system with an A1 rating would have the highest security rating under the Orange Book system (Oz, 2000). (See Department of Defense, 1985, to retrieve the full text of the Orange Book standards.)

Critics of the Orange Book standards complain that the ratings deal with secrecy and access only, ignoring protection against other types of system damage. They also note that the Orange Book does not address network security (Oz, 2000). These limitations and others led to the development of a set of IT security criteria that would provide "a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation" (Oz, 2000). They were published in 1999 by the International Organization for Standardization (ISO), as ISO Standard 15408 (titled Information Technology—Security Techniques—Evaluation Criteria for IT Security). They are now also published by Common Criteria under the title Common Criteria for Information Technology Security Evaluation (CC), Version 2. (The full text may be obtained from Common

Criteria, 2004). These criteria allow an organization to use a common set of requirements and thus to compare the results of independent security evaluations.

Physical Safeguards

A security program must address physical as well as technical and administrative safeguards. Physical safeguards involve protecting the actual computer hardware, software, data, and information from physical damage or loss due to natural, human, or environmental threats. Several specific issues related to physical security are addressed in this section (Lee, in press):

- Assigned security responsibility
- Media controls
- Physical access controls
- Workstation security

Assigned Security Responsibility

Each component of the health care information system should be secure, and one easily identifiable employee should be responsible for that security. These individuals are in turn accountable to the chief security officer. For example, in a nursing department the department manager might be responsible for ensuring that all employees have been trained to understand and use security measures and that they know the importance of maintaining the security of patient information. The network administrator, however, might be the person responsible for assigning initial passwords and removing access from terminated employees or employees who transfer to other departments.

Media Controls

The physical media on which health information is stored must be physically protected. Media controls are the policies and procedures that govern the receipt and removal of hardware, software, and computer media such as disks and tapes into and out of the organization and also their movements inside the organization.

Media controls also encompass data storage. Backup tapes, for example, must be stored in a secure area with limited access. The final disposition of electronic media is another aspect of media controls. Policies for the destruction of patient information must address the electronic media and hardware (workstations and servers) that contain patient information. As organizations gather old computers, all patient data must be removed before this equipment goes to surplus or is otherwise disposed of.

Physical Access Controls

Physical access controls are designed to limit physical access to health information to persons authorized to see that information. Locks and keys are examples of physical access controls. However, it is obvious that all workstations cannot be kept under lock and key. This might create a secure system, but it would not be readily available to the health care providers who need patient information. Some of the physical access control components that can be employed are equipment control; a facility security plan; procedures that verify user identity before allowing physical access to an area; a procedure for maintaining records of repairs and modifications to hardware, software, and physical facilities; and a visitor sign-in procedure. Organizations should have a system, such as an inventory control system, that tells them exactly what equipment is currently in use in their health care information system. An inventory control system generally involves marking or tagging each piece of equipment with a unique number and assigning each piece to a location and a responsible person. When equipment is moved, retired, or destroyed, that action must be documented in the inventory control system. Another form of equipment control is to install antitheft devices, such as chains that attach computers to desks, alarms, and other tools that deter thieves.

A facility security plan is a plan that ensures that the individuals in a certain area are authorized to have access to that area. The main computer operations of a health care organization will generally be under tight security, including video surveillance and personal security checks. Badges with photographs are common in health care facilities to help identify personnel who are authorized to access certain buildings and facilities. Some secure areas require individuals to punch a code into a keypad or swipe an identification card over a card reader before entry is allowed. The facility security plan should also have procedures for admitting visitors. Each visitor might sign in and be issued a temporary identification badge, for example. There may be areas of the organization that are not open to visitors at all.

Workstation Security

Workstations that allow access to patient information should be placed in areas that are secure or monitored at all times. The workstations in the reception area or other public areas should be situated so that visitors or others cannot read the screen. Devices can be placed over workstation monitors that prevent people from reading the screen unless they are directly in front of it. Another aspect of workstation security is developing clear policies for workstation use. These policies should delineate, among other things, the appropriate functions to perform on the workstation and rules for sharing workstations.

Organizations that allow personnel to work from home have additional workstation security issues. Employees working from home must be given clear guidance on appropriate use of the organization's computer resources, whether these resources

involve hardware, software, or Web access. Employees should access any patient-identifiable information through a secure connection, with adequate monitoring to ensure that the user is in fact the authorized employee.

All the aspects of physical security require adequate training of all personnel with potential access to the health care information systems. Employees, agents, and contractors with access to locations that house patient information must all participate in security and confidentiality awareness education.

Technical Safeguards

Many different technical safeguards can be used to help secure health care information systems and the networks on which they reside. Again, we will not provide a comprehensive list of all available safeguards, but will present a few representative examples. We will discuss technical safeguards related to the following topics (Lee, in press):

- Access control
- Entity authentication
- Audit trails
- Data encryption
- Firewall protection
- Virus checking

Access Control

Only individuals with a *need to know* should have access to patient-identifiable health information. Modern computer systems, including databases and networks, allow users to access a variety of resources such as individual files, database files, and tapes and to use printers and other peripheral devices. This sharing of resources is an important component of effective health care information systems, but it requires that network administrators and database administrators set appropriate access rights for each resource. Often users of a health care information system have to be assigned network access rights and separate application access rights before they can use the system.

Control over access to health data may make use of any one of the following methods:

- User-based access
- Role-based access
- Context-based access

Before we discuss each of these options, a brief explanation of access rights is necessary. Traditional user-based and role-based access rights have two parameters—who and how. The *who* is a list of the users with rights to access the information or computer resource in question. This list, called an *access control list*, may be organized by individual users or by groups of users. These groups are generally defined by role or job function. For example, all coders in the health information management department would be granted the same access rights, all registered nurses in a particular job classification would be granted the same access, and so forth.

The *how* parameter of the access control scheme specifies how a user may access the resource. Typical examples of the actions users might be allowed to take are read, write, edit, execute, append, and print. Only so-called owners and administrators will be granted full rights so that they can modify or delete or create new components for the resource. Clearly, owner and administrative privileges for the use of health care information systems should be carefully monitored.

User-based access is defined as “a security mechanism used to grant users of a system access based upon the identity of the user.” With *role-based access control* (RBAC), access decisions are based on the roles individual users have within the organization. “With RBAC, rather than attempting to map an organization’s security policy to a relatively low-level set of technical controls (typically, access control lists), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform the role” (63 Fed. Reg. 155, August 12, 1998). One of the benefits of role-based over user-based access is that as new applications are added, privileges are more easily assigned. Discretionary assignment of access by an administrator is limited with RBAC. Users must be assigned to a specific role in order to be assigned access to a specific application.

Context-based access control is the most stringent of the three options. Harry Smith (2001) describes it this way: “A context-based access control scheme begins with the protection afforded by either a user-based or role-based access control design and takes it one step further. . . . Context-based access control takes into account the person attempting to access the data, the type of data being accessed and the *context* of the transaction in which the access attempt is made.” In other words the context-based access has three parameters to consider—the who, the how, and the context in which the data are to be accessed. The following example illustrates the differences among the three types of access control.

Mary Smith is the director of the Health Information Management Department in a hospital. Under a user-based access control scheme, Mary would be allowed read-only access to the hospital’s laboratory information system because of her personal identity—that is, because she is Mary Smith and uses the proper log-in and password(s) to get into the system. Under a role-based control scheme, Mary would be allowed read-only access to her hospital’s lab system because she is part of the Health Information Management Department and all department employees have been granted

read-only privileges to this system. If the hospital were to adopt a context-based control scheme, Mary might be allowed access to the lab system only from her own workstation or another workstation in the Health Information Services Department, provided she used her proper log-in and password. If she attempted to log in from the Emergency Department or another administrative office, she might be denied access. The context control could also involve time of day. Because Mary is a daytime employee, she might be denied access if she attempted to log in at night.

Entity Authentication

Access control mechanisms are effective means of controlling who gains entry to a health care information system only when there is a system for ensuring the identity of the individual attempting to gain access. *Entity authentication* is defined in the HIPAA Security Rule as “the corroboration that a person is the one claimed.” Entity authentication associated with health care information systems should include at least (1) automatic log-off and (2) a unique user identifier.

Automatic log-off is a security procedure that causes a computer session to end after a predetermined period of inactivity, such as ten minutes. Multiple software products are available that allow network administrators to set automatic log-off parameters. Once installed, these log-off systems act like any other screen saver on a typical workstation, coming on after a set period of inactivity. Users are then required to enter a network password to deactivate the log-off system screen. Generally, a device driver is also installed that prevents rebooting to deactivate the log-off system. Other security measures that may be included in automatic log-off products are features that prevent users from changing the screen saver and that allow an authorized person to set local password options in case the user is not connected to the network. Failed log-in attempts may be recorded and reported on, along with statistics on user log-ins, elapsed time, and user identification.

Each user of a health care information system must be assigned a *unique identifier*. This identifier is a combination of characters and numbers assigned and maintained by the security system. It is used to track individual user activity. This identifier is commonly called the *user ID* or *log-on ID*. It is the *public*, or known, portion of most user log-on procedures. For example, many organizations will assign a log-on identifier that is the same as the user’s e-mail address or a combination of the user’s last and first name. It is generally fairly easy to identify a user by his or her log-on. John Doe’s log-on identifier might be “doej,” for example. Because of the public nature of the log-in, additional safeguards, beyond the log-on ID, are needed.

Entity authentication can be implemented in a number of different ways in a health care information system. The most common entity authentication method is a *password system*. Other mechanisms include *personal identification numbers (PINs)*, *biometric identification systems*, *telephone callback systems*, and *tokens*. These implementation methods

can be used alone or in combination with other systems. Security experts often encourage *layered* security systems that use more than one security mechanism. As one security expert has stated, “A series of overlapping solutions works much more effectively, even when you know the solutions are individually fallible. If you line up three security controls that are each 60 percent effective, together they’re something like 90 percent effective against a given attack” (Briney, 2000).

Walsh (2003) recommends a system that uses a *two-factor* authentication. He identifies these three methods for authentication, and any two of them used together would constitute a two-factor system:

- Something you know, such as a password or personal identification number (PIN)
- Something you have, such as an ATM card, token, or swipe card
- Something you are, such as a biometric fingerprint, voice scan, or iris or retinal scan [Walsh, 2003].

Password Systems. The most common way to control access to a health care information system (or any other computer system for that matter) is through a combination of the user ID and a password or PIN. User IDs and passwords for a system are maintained either as a part of the access control list for the network or local operating system or in a special database. The list or database is then searched for a match before the user is allowed to access the system requested. While the user ID is not secret, the password or PIN is. Passwords are generally stored in an encrypted form for which no decryption is available (White, 2001; Oz, 2000).

Although password and PIN systems are the most common forms of entity authentication, they also provide the weakest form of security. A *password* is defined by Whatis?com (2002) as an “unspaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user.” Typically, a password is made up of four to sixteen characters. One of the biggest problems with passwords is that users may share them or publicly display them. Users will often write down passwords they cannot remember. They may even tape or post the password on the computer workstation. Health care organizations must take steps to prevent this type of password misuse. Clear policies on the use and maintenance of passwords, employee education, and meaningful sanctions for policy violators are essential.

Another common problem with passwords is that when they are simple enough to remember, they may be simple enough for someone else to guess. Passwords are encrypted, but there are software programs available, called *password crackers*, that can be used to identify an unknown or forgotten password. Unfortunately, unauthorized persons seeking to gain access to computer systems can also use these applications (White, 2001; Whatis?com, 2002). Health care organizations should establish enforceable, clear guidelines for choosing passwords. Here are some suggestions (White, 2001; Whatis?com, 2002; Lee, in press):

Perspective: Password Do's and Don'ts

DON'T

- Pick a password that someone who knows you can easily guess (for example, do not use your Social Security Number, birthday, maiden name, pet's name, child's name, or car name).
- Pick a word that can be found in the dictionary (because cracker programs can rapidly try every word in the dictionary!).
- Pick a word that is currently newsworthy.
- Pick a password that is similar to your previous password.
- Share your password with others.

DO

- Pick a combination of letters and at least one number. Pick a password with at least eight characters, mixing uppercase and lowercase if your password system is case sensitive.
- Pick a word that you can easily remember.
- Change your password often. (Some networks require that you change your password periodically.)

Biometric Identification Systems. Because of the inherent weaknesses of password systems, other identification systems have been developed. Biometric identification systems employ users' biological data, in the form, for example, of a voiceprint, fingerprint, handprint, retinal scan, faceprint, or full body scan. Although some sources (White, 2001) call biometric identification systems the "wave of future," there are indications that the technology is not yet widely used. The 2001 *Information Security* survey found that nearly half of the respondents had no plans to acquire biometrics for network access control (Briney, 2001).

Nevertheless, biometrics is likely to play an increasing role in health care information system security. Biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and a database that stores the biometric data for comparison. IBM, Microsoft, Novell, and other computer companies are currently working on a standard for biometric devices, called BioAPI. This standard will allow software products from different manufacturers to interact with one another (Whatis?com, 2002).

Telephone Callback Procedures. Telephone callback procedures are another form of entity authentication in use today. Callback is used primarily when employees have access to a health care information system from home. When a modem dials into the

system, a special callback application asks for the telephone number from which the call has been placed. If this number is not an authorized number, the callback application will not allow access (Oz, 2000).

Tokens. Tokens are devices, such as key cards, that are inserted into doors or computers. With token authentication systems, identification is based on the user's possession of the token (Eng, 2001). The disadvantage of tokens is that they can be lost, misplaced, or stolen. When tokens are used in combination with a password or PIN, it is essential that the password or PIN not be written on the token or in a location near where the token is stored.

Audit Trails

Webopedia.com (2004a) defines an *audit trail* as “a record showing who has accessed a computer system and what operations he or she has performed during a given period of time. In addition, there are separate audit trail software products that enable network administrators to monitor use of network resources.” Audit trails are generated by specialized software, and they have multiple uses in securing information systems. These uses may be categorized as follows (Gopalakrishna, 2000):

- *Individual accountability.* When employees' or other individuals' actions are tracked with an audit trail these individuals become accountable for their actions, which can be a strong deterrent to violating acceptable policies and procedures.
- *Reconstructing electronic events.* Audit trails can also be used to reconstruct how and when a computer or application was used. This can be quite useful when there is a suspected security breach, whether internal or external.
- *Problem monitoring.* Some types of auditing software can detect problems such as disk failures, overutilization of system resources, and network outages as they occur.
- *Intrusion detection.* When there are attempts to gain unauthorized access to a system an audit system can detect them.

Data Encryption

Data encryption is used to ensure that data transferred from one location on a network to another are secure from anyone eavesdropping or seeking to intercept them. This becomes particularly important when sensitive data, such as health information, are transmitted over public networks such as the Internet or across wireless networks. Secure data are data that cannot be intercepted, copied, modified, or deleted.

Cryptography is the study of encryption and decryption techniques. It is a complicated science with a vast number of associated techniques. Only the basic concepts and some current authentication technologies will be discussed in this chapter. Public Key

Infrastructure and Pretty Good Privacy are forms of encryption being used in health care today. They are used to authenticate the sender and receiver of messages transmitted over networks, particularly when the Internet is involved in the data transmission.

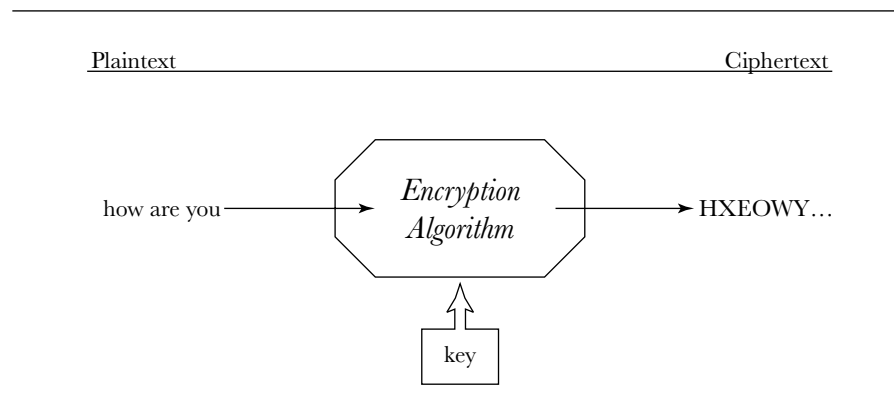
Some basic terms associated with encryption are *plaintext*, *encryption algorithm*, *ciphertext*, and *key*. Plaintext refers to data before any encryption has taken place. In other words, the original datum or message is recorded in the computer system as plaintext. An encryption algorithm is a computer program that converts plaintext into an enciphered form. The ciphertext is the data after the encryption algorithm has been applied. The key in an encryption and decryption procedure is unique data that is needed both to create the ciphertext and to decrypt the ciphertext back to the original message. Figure 10.3 is a simple diagram of the components of an encryption and decryption system (White, 2001).

The earliest encryption systems used a single, private key. In other words, the same key (or code) was used to generate the ciphertext and to decrypt it. The problems with the single, private (secret) key systems were that both the sender and receiver had to have the key and that this key had to be protected from interception or tampering as well.

Public Key Infrastructure. *Public key cryptography* addresses the basic problems of single, private key systems. In a public key system, there are two keys, a *private key* and a *public key*. Basically, in this two-key system, data encrypted with the public key can be decrypted only by the private key, and data encrypted by the private key can be decrypted only by the public key. With public key cryptography, encrypted data become very difficult to break (White, 2001). The following is a simplistic illustration of how public key cryptography works.

A health care clinic in a major city needs to send patient information to the main hospital across town. First, the hospital sends a public key to the clinic and it keeps the corresponding private key in a secure location. The clinic uses the public key to

FIGURE 10.3. ENCRYPTION PROCEDURE.



encrypt the data before sending it over to the hospital. Now, only the hospital can decode the data, because it has sole possession of the corresponding private key.

Public key cryptography today is a component of Public Key Infrastructure (PKI), an entire system designed to make the use of public key cryptography practical. PKI is a combination of encryption techniques, software, and services. A health care organization can adopt an in-house PKI model or contract with an application service provider (ASP) to host and manage a PKI system for it. One potential use of PKI in health care is sending secure e-mail. To send a secure e-mail in the PKI environment, the sender retrieves the recipient's public key from a directory in his or her organization. After obtaining the public key, the sender encrypts the e-mail message (by selecting the "encrypt" button, for example) and sends the encrypted message. When the e-mail arrives at the recipient's computer, the recipient's private key will automatically decrypt the message (Etheridge, 2001).

There are other potential uses for PKI technology in health care, such as ensuring secure access to Web-based health records or other health care information systems. One example is that Marconi Medical Systems, which makes a picture archiving and communications system (PACS), is integrating PKI into its Web-based products to allow remote access through a standard Web browser. PKI is also being used by an on-line prescription service (Etheridge, 2001). As wonderful as PKI sounds, it has some problems. It is expensive, and many of the systems are proprietary and will not interact with other systems. However, with the HIPAA standards demanding a higher level of security for on-line health care transactions, the use of PKI technology in health care is likely to increase.

Pretty Good Privacy. In the early 1990s, software engineer Phillip Zimmermann created open source encryption software that he called Pretty Good Privacy. PGP has the specific purpose of allowing the average person to create and send secure e-mail and data files. PGP uses public key cryptography and digital signatures. In order to use PGP, both the sending and the receiving workstations must have the same PGP software. Originally, PGP was available via the Internet. A freeware version is available to individuals in the United States from the PGP Corporation (www.pgp.com), and PGP can also be purchased for commercial use (White, 2001).

Firewall Protection

A *firewall* is "a system or combination of systems that supports an access control policy between two networks" (White, 2001). The term *firewall* may be used to describe software that protects computing resources or to describe a combination of software, hardware, and policies that protects these resources (Oz, 2000; Whatis?com, 2002). The most common place to find a firewall is between the health care organization's internal network and the Internet. This firewall prevents users who are accessing the

health care network via the Internet from using certain portions of that network and also prevents internal users from accessing various portions of the Internet (Oz, 2000; Whatis?com, 2002).

The basic types of firewalls are (1) *packet filter*, or network level, and (2) *proxy servers*, or application level. The packet filter firewall is essentially a router that has been programmed to filter out some types of data and to allow other types to pass through. The early versions of these firewalls were fairly easy to fool. As routers have become more sophisticated, the protection offered by this type of firewall has increased. The proxy server is a more complex firewall device. The proxy server firewall is software that runs on a computer that acts as the *gatekeeper* to an organization's network. Any external transaction enters the organization's network through the proxy server. The request for information is actually "stopped" at the proxy server, where a proxy application is created. This proxy is what goes into the organization's network to retrieve the requested information (White, 2001).

As important as firewalls are to the overall security of health care information systems, they cannot protect a system from all types of attacks. Many viruses, for example, can hide inside documents that will not be stopped by a firewall.

Virus Checking

Computer viruses come in many different varieties. The common types may be classified as (Whatis?com, 2002)

- *File infectors*, which attach to program files so that when a program is loaded the virus is also loaded
- *System or boot-record infectors*, which infect system areas of diskettes or hard disks
- *Macro viruses*, which infect Microsoft Word applications, inserting unwanted words or phrases

A *worm* is a special type of computer virus that stores and then replicates itself. Worms usually transfer from computer to computer via e-mail. A Trojan horse is a destructive piece of programming code that hides in another piece of programming code that looks harmless, such as a macro or e-mail message (White, 2001).

Fortunately, there are effective antivirus software packages on the market today. These programs have three main features: *signature-based scanning*, *terminate-resident monitoring*, and *multilevel generic scanning*.

Signature-based scanning works by recognizing the unique pattern, or signature, of a virus. As new viruses appear, the antivirus program developers catalogue their signatures. The signature scanning feature of the antivirus software then scans applications, messages, and files as they are downloaded or opened, searching for matches to the signatures in the catalogue. Some types of viruses are designed to avoid

detection by the signature scanning feature. Terminate-and-stay-resident antivirus software runs in the background while an application runs in the foreground. It is useful for finding hard-to-detect viruses such as stealth viruses and polymorphic viruses. A third feature of most antivirus packages is multilevel generic scanning. This type of virus checking employs “expert” analysis techniques to catch viruses the other two features might miss (White, 2001).

Virus checking is an important component of a health information security program. As discussed earlier, virus attacks are very common and can cause extensive damage and loss of productivity. Antivirus software is effective as long as the virus catalogue is updated frequently. Most antivirus software packages can be set to automatically scan the user’s computer system periodically to detect and clean any viruses found.

Security in a Wireless Environment

As discussed in earlier chapters, wireless technologies are changing the way health care information systems operate. The adoption of wireless technologies has been relatively rapid, creating concerns about the level of security they offer in an environment like the health care organization. According to a recent white paper written by Fluke Networks (2003, p. 1), the issues related to wireless security are “exactly the same as with wired security. The problem with wireless is that it’s difficult to limit the transmission media to just the areas that we control, or just the hosts we want on our network.”

In the standard for the most common form of wireless network (IEEE Standard 802.11), there is a specification for encryption called Wired Equivalent Privacy (WEP). WEP has been reported to be flawed and not adequate for situations involving sensitive information (such as health care) (Fluke Networks, 2003). Fortunately, other encryption methods are being developed for use in the wireless environment. Encryption, however, is optional, and not all organizations with wireless networks employ it. In one recent test, a user was able to pick up 200 wireless access points during an average day’s driving in the Seattle, Washington, area, and only 34 percent of them were encrypted (Fluke Networks, 2003). (We can only hope that this 34 percent represents all the area’s health care organizations!)

Health care organizations that use wireless technologies should pay close attention to risk analysis for them and include safeguards as a part of ongoing risk management. As with other networks and information systems, the organization must know where the threats and vulnerabilities are.

Securing the handheld devices and laptop computers commonly associated with a wireless network also poses challenges for the health care organization. Clear policies, and appropriate sanctions for those violating the policies, should be established governing the downloading of patient-specific information onto personal devices such as

these. In addition to the standard inventory control mechanisms and assigning responsibility for portable computers, health care organizations may want to provide their employees with accessories that could minimize theft. For example (Hughes, 2000):

- Cases that do not appear to contain computers.
- Cables with locks that hook onto tables; once this cable is removed from the computer, an unauthorized person cannot turn the computer on.
- Alarms and software that “instruct” the computer to call and “report” its location.

Summary

Health information is created, maintained, and stored using computer technology. The use of this technology creates new issues in protecting patients’ rights to privacy and confidentiality, and demands that health care organizations develop comprehensive information security programs. The publication of the final HIPAA Security Rule in 2003 underscores the importance of securing health information and the need for comprehensive security programs. The standards and specifications of the HIPAA rule can serve as a framework for health care organizations as they design their individual security programs.

Information security programs need to be designed to address internal and external threats to health care information systems, whether those threats are intentional or unintentional. Health information security programs should address administrative, physical, and technical safeguards. This chapter not only outlined the HIPAA security requirements but also provided a discussion of many of the common security measures that can be employed to minimize potential risks to health information.

Chapter Ten: Learning Activities

1. Do an Internet or library search for recent articles discussing the HIPAA Security Rule. From your research, write a short paper discussing the impact of these security regulations on health care organizations. How have these regulations changed the way organizations view security? Do you think the regulations are too stringent? Not stringent enough? Just right? Explain your rationale.
2. Interview a chief security officer at a hospital or other health care facility. What are the major job responsibilities of this individual? To whom does he or she report within the organization? What are the biggest challenges of the job?
3. Contact a physician’s office or clinic, and ask if the organization has a security plan. Discuss the process that staff undertook to complete the plan, or develop an outline of a plan for them.



PART FOUR

SENIOR MANAGEMENT IT CHALLENGES



CHAPTER ELEVEN

ORGANIZING INFORMATION TECHNOLOGY SERVICES

By now you should have an understanding of health care data, the various clinical and administrative applications that are used to manage data, and the processes of selecting, acquiring, and implementing health care information systems. You should also have a basic understanding of the core technologies that are common to many health care applications and appreciate some of what it takes to ensure that information systems are reliable and secure.

In many health care organizations an information technology (IT) function employs staff who are involved in these and other IT-related functions—everything from customizing a software application to setting up and maintaining a wireless network to performing system backups. In a solo physician practice, this responsibility may lie with the office manager or lead physician. In a large hospital setting, this responsibility may lie with the IT department in conjunction with the medical staff, administration, and the major departmental units—for example, admissions, finance, radiology, and nursing.

Some health care organizations outsource a portion or all of their IT services; however, they are still responsible for ensuring that IT services are of high quality and support the IT needs of the organization. This responsibility cannot be delegated entirely to an outside vendor or information technology firm. Health care executives must manage information technology resources just as they do human, financial, and other facility resources.

This chapter provides an overview of the various functions and responsibilities that one would typically find in the IT department of a large health care organization.

We describe the different groups or units that are typically seen within an IT department. We review a typical organizational structure for IT and discuss the variations that are often seen in that structure and the reasons for this variation. This chapter also presents an overview of the senior IT management roles and the roles with which health care executives will often work in the course of projects and IT initiatives. IT outsourcing, in which the health care organization asks an outside vendor to run IT, is reviewed. Finally, we examine approaches to evaluating the efficiency and effectiveness of the IT department.

Information Technology Functions

The IT department has been an integral part of most hospitals or health care systems since the early days of mainframe computing. If the health care facility was relatively large, complex, and used a fair amount of information technology, one would find IT staff “behind the scenes” developing or enhancing applications, building system interfaces, maintaining databases, managing networks, performing system backups, and carrying out a host of other IT support activities. Today the IT department is becoming increasingly important, not only in hospitals but in all health care organizations that use IT to manage clinical and administrative data and processes.

Throughout this chapter we refer to the IT department typically found in a large community hospital or health care system. We chose this setting because it is typically the most complex and IT intensive. However, many of the principles that apply to managing IT resources in a hospital setting also apply to other types of health care facilities, such as an ambulatory care clinic or rural community health center. The breadth and scope of the services provided may differ considerably, however, depending on the extent to which IT is used in the organization.

Responsibilities

The IT department has several responsibilities:

- Ensuring that an IT plan and strategy have been developed for the organization and that the plan and strategy are kept current as the organization evolves; these activities are discussed in Chapter Twelve.
- Working with the organization to acquire or develop and implement needed new applications; these processes were discussed in Chapters Six and Seven.
- Providing day-to-day support of users: for example, fixing broken personal computers, responding to questions about application use, training new users, and applying vendor-supplied upgrades to existing applications.

- Managing the IT infrastructure: for example, performing backups of databases, installing network connections for new organizational locations, printing weekly paychecks, and securing the infrastructure from virus attacks.
- Examining the role and relevance of emerging information technologies.

Core Functions

To fulfill their responsibilities, all IT departments have four core functions. Depending on the size of the IT group and the diversity of applications and responsibilities, there may be several subsidiary departments or subgroups for each function.

Operations and Technical Support. The operations and technical support function manages the IT infrastructure—for example, the servers, networks, operating systems, database management systems, and workstations. This function installs new technology, applies upgrades, troubleshoots and repairs the infrastructure, performs “housekeeping” tasks such as backups, and responds to user problems, such as a printer that is not working.

Within this function, there can be several IT subgroups:

- *Data center management:* manages the equipment in the organization’s computer room.
- *Network engineers:* manage the organization’s network technologies.
- *Server engineers:* oversee the installation of new servers, and perform such tasks as managing server space utilization.
- *Database managers:* add new databases, support database query tools, and respond to database problems such as file corruptions.
- *Security:* ensure that virus protection software is current, physical access to the computer room is constrained, disaster recovery plans are current, and processes are in place to manage application and system passwords.
- *Help desk:* provide support to users who call in with problems such as broken office equipment, trouble with operating an application, a forgotten password, or uncertainty about how to perform a specific task on the computer.
- *Deployments:* install new workstations and printers, move workstations when groups move to new buildings, and the like.
- *Training:* train organization staff on new applications and office software, such as presentation development applications.

Applications Management. The applications management group manages the processes of acquiring new application systems, developing new application systems, implementing these new systems, providing ongoing enhancement of applications,

troubleshooting application problems, and working with application suppliers to resolve these problems.

Within this function there can be several IT departments or groups:

- Groups may be established that focus on major classes of applications: for example, a financial systems group and a clinical systems group.
- Large organizations may have groups dedicated to specific applications: for example, a group to support the applications in the clinical laboratory or in radiology.
- Organizations that perform a significant amount of internal development may have an applications development group.
- Organizations, regardless of size, may have groups that focus on specific types of internal development: for example, a Web development group.

Specialized Groups. Health care organizations may develop groups that have very specialized functions, depending on the type of organization or the organization's approach to IT. For example:

- Academic medical centers may have a group that supports the needs of the research community.
- Organizations that engage in a significant degree of process reengineering during application implementation may have a process redesign group.
- Decision-support groups are sometimes created to help users and management perform analyses and create reports from corporate databases: for example, quality-of-care reports or financial performance reports.

In addition, the chief information officer (CIO) is often responsible for managing the organization's telecommunications function—the staff who manage the phone system, overhead paging system, and nurse call systems. Depending on the organization's structure and the skill and interests of the CIO, one occasionally finds these organizational functions reporting to the CIO:

- The health information management or medical records department
- The function that handles the organization's overall strategic plan development
- The marketing department

IT Administration. Depending on the size of the IT department, one may find groups that focus on supporting IT administrative activities. These groups may perform such tasks as

- Overseeing the development of the IT strategic plan
- Developing and monitoring the IT budget

- Providing human resource support for the IT staff
- Providing support for the management of IT projects: for example, developing project status reports or providing project management training
- Managing the space occupied by an IT department or group

A typical organizational structure for an IT department in a large hospital is shown in Figure 11.1.

IT Senior Leadership Roles

Within the overall IT group, several positions and roles are typically present. These roles range from senior leadership—for example, the chief information officer (CIO)—to staff who do the day in, day out work of implementing application systems—for example, systems analysts. In the following sections, we will describe several senior-level IT positions, including the

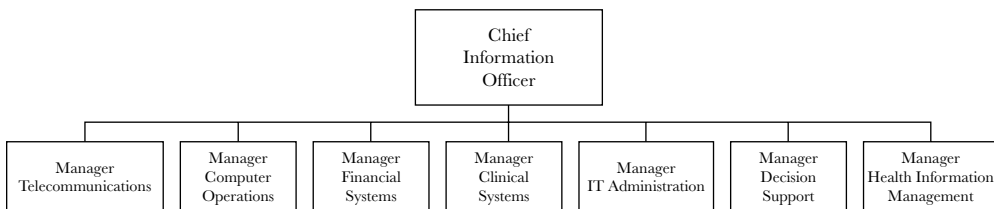
- Chief information officer (CIO)
- Chief technology officer (CTO)
- Chief security officer (CSO)
- Chief medical informatics officer (CMIO)

This is not an exhaustive list of all possible senior-level positions, but the discussion provides an overview of typical roles and functions.

The Chief Information Officer. Many midsize and large health care organizations employ a *chief information officer* (CIO). The CIO not only manages the IT department but is also seen as the executive who can successfully lead the organization in its efforts to apply IT to advance its strategies.

Surveys of health care organizations, such as those conducted by the College of Healthcare Information Management Executives (CHIME), have chronicled the

FIGURE 11.1. TYPICAL IT ORGANIZATION CHART.



evolution of the health care CIO (CHIME, 1998). This evolution has involved debates on CIO reporting relationships, salaries, and titles and the role of the CIO in an organization's strategic planning.

A good CIO can be a significant asset to an organization. The CIO can

- Be a major contributor to the organization's strategy development, and apply business thinking and strategy formation skills that extend beyond his or her IT responsibilities.
- Help the organization understand the potential of IT to make real and significant contributions to the organization's plans, activities, and operations.
- Be a leader, motivator, recruiter, and retainer of superior IT talent.
- Ensure that the IT infrastructure is robust, effective, efficient, and sustained.
- Ensure that the IT organization runs effectively and efficiently.

Earl and Feeney (1995) conducted a comprehensive study of CIOs in a wide range of industries who "added value" to their respective organizations. They found that the value-added CIOs

- Obsessively and continuously focus on business imperatives so that they focus the IT direction correctly.
- Have a track record of delivery that causes IT performance problems to drop off management's agenda.
- Interpret for the rest of the leadership the meaning and nature of the IT success stories of other organizations.
- Establish and maintain good working relationships with the members of the organization's leadership.
- Establish and communicate the IT performance record.
- Concentrate the IT development efforts on those areas of the organization where the most leverage is to be gained.
- Work with the organization's leadership to develop a shared vision of the roles and contributions of IT.
- Make important general contributions to business thinking and operations.

Earl and Feeney (1995) also found that the value-added CIO, as a person, has integrity, is goal directed, is experienced with IT, and is a good consultant and communicator. Those organizations that have such a CIO tend to describe IT as critical to the organization, find that IT thinking is embedded in business thinking, note that IT initiatives are well focused, and speak highly of IT performance.

Organizational excellence in IT doesn't just happen. It is managed and led. If the health care organization decides that the effective application of IT is a major element

of its strategies and plans, it will need a very good CIO. Failure to hire and retain such talent will severely hinder the organization's aspirations.

Whom the CIO should report to has been a topic of industry debate and an issue inside organizations as well. CIOs will often argue that they should report to the chief executive officer (CEO). This argument is not wrong nor is it necessarily right. The CIO does need access to the CEO and clearly should be a member of the executive committee and actively involved in strategy discussions. However, the CIO needs a boss who is a good mentor, provides appropriate political support, and is genuinely interested in the application of IT. Chief financial officers (CFOs) and chief operating officers (COOs) can be terrific in these regards. In general about one-third of all health care provider CIOs report to the CEO, one-third report to the CFO, and one-third report to the COO.

The Chief Technology Officer. The *chief technology officer* (CTO) has several responsibilities. The CTO must guide the definition and implementation of the organization's technical architecture. This role includes defining technology standards (for example, setting out the operating systems and network technologies the organization will support), ensuring that the technical infrastructure is current (for example, that major vendor releases and upgrades have been applied), and ensuring that all the technologies *fit*. The role of ensuring fit is similar to the role of the architect of a house in ensuring that the materials used to construct a house come together in a way that results in the desired house.

The CTO is also responsible for tracking emerging technologies, identifying those new technologies that might provide value to the organization, assessing those technologies, and when appropriate, working with the rest of the IT department and the organization to implement these technologies. For example, the CTO may be asked to investigate the role of the new biometric security technologies. The CTO role is not often found in smaller organizations but is increasingly common in larger ones. In smaller organizations, the CIO also wears the CTO hat.

The Chief Security Officer. As discussed in Chapter Ten, *chief security officer* (CSO) is a relatively new position that has emerged as a result of the growing threats to information security and the health care organization's need to comply with HIPAA security regulations. The primary role and functions of the CSO are to ensure that the health care organization has an effective information security plan, that appropriate technical and administrative procedures are in place to ensure that information systems are secure and safe from tampering or misuse, and that appropriate disaster recovery procedures exist.

The Chief Medical Informatics Officer. Like CSO, *chief medical informatics officer* (CMIO) is a relatively new position. The CMIO position emerged as a result of the growing interest in adopting clinical information systems and the need for physician

leadership in this area. The CMIO is usually a physician, and this role can be filled through a part-time commitment by a member of the organization's medical staff.

Examples of the types of responsibilities a CMIO might assume include

- Leading the implementation of an electronic medical record (EMR) system for a health care organization
- Engaging physicians and other health care professionals in the development and use of the EMR system
- Leading the clinical informatics steering committee or other designated group that serves as the central governance forum for establishing the organization's clinical IT priorities
- Keeping a pulse on national efforts to develop electronic health record (EHR) systems, and assuming a leadership role in areas where the national effort and the organization's agenda are synergistic
- Being highly responsive to user needs, such as training, to ensure widespread use and acceptance of clinical systems

The CIO, CTO, CSO, and CMIO all play important roles in helping to ensure that information systems acquired and implemented are consistent with the strategic goals of the health care organization, are well accepted and effectively used, and are adequately maintained and secured. Sample job descriptions for the CIO and the CMIO positions are displayed in Figures 11.2 and 11.3.

More IT Staff Roles

The IT leadership team cannot unilaterally carry out the organization's IT agenda. The department's work relies heavily on highly trained, qualified professional and technical staff to perform a host of IT-related functions. Here are brief descriptions of some key professionals who work in IT:

- The system analyst
- The programmer
- The database administrator
- The network administrator
- The telecommunications specialist
- Other IT staff

The System Analyst. The role of the *system analyst* will vary considerably depending on the analyst's background and the needs of the organization. Some analysts have a strong computer programming background, whereas others have a business orientation or come from one of the clinical disciplines, such as nursing, radiology, or laboratory sciences.

Most system analysts work closely with managers and end users in identifying information system needs and problems, evaluating workflow, and determining strategies for optimizing the use and effectiveness of particular systems. They may specify the inputs to be accessed by a system, design the processing steps, and format the output to meet users' needs.

When an organization decides to implement a new information system, systems analysts are often called upon to determine what computer hardware and software will be needed. They prepare specifications, flowcharts, and process diagrams for computer programmers to follow. They work with programmers to *debug*, or eliminate, errors in the system. Systems analysts may also conduct extensive testing of systems, diagnose problems, recommend solutions, and determine whether program requirements have been met. They may also prepare cost-benefit and return-on-investment analyses to help management decide whether implementing a proposed system will be financially attractive.

The Programmer. In some organizations the system analyst and the computer *programmer* fulfill similar roles, particularly if the analyst has a strong programming background. However, many system analysts do not have such experience, yet they work closely with programmers.

Programmers write, test, and maintain the programs that computers must follow to perform their functions. They also conceive, design, and test logical structures for solving problems with computers. Many technical innovations in programming—advanced computing technologies and sophisticated new languages and programming tools—have redefined the role of a programmer and elevated much of the programming work done today (Department of Labor, Bureau of Labor Statistics, 2004).

Programmers are often grouped into two broad types—applications programmers and systems programmers. *Applications programmers* write programs to handle specific user tasks, such as a program to track inventory within an organization. They may also revise existing packaged software or customize generic applications such as integration technologies or utilities that manage a user's desktop. *Systems programmers* write programs to maintain and control infrastructure software, such as operating systems, networked systems, and database systems. They are able to change the sets of instructions that determine how the network, workstations, and central processing units within a system handle the various jobs they have been given and how they communicate with peripheral equipment such as other workstations, printers, and disk drives.

The Database Administrator. *Database administrators* work with database management systems software and determine ways to organize and store data. They identify user requirements, set up computer databases, and test and coordinate modifications to these systems. An organization's database administrator ensures the performance of the database systems, understands the platform on which the databases run, and

FIGURE 11.2. SAMPLE CIO JOB DESCRIPTION.

<<XX>> HEALTH CARE SYSTEM, INC. JOB DESCRIPTION

POSITION TITLE: Chief Information Officer (CIO)

DEPARTMENT: Information Systems & Telecommunications

POSITION REPORTS TO: Chief Financial Officer (CFO)

POSITION SUPERVISES: Information Systems Department, Telecommunications Department

POSITION REQUIREMENTS:

Master's of Science Degree in Information Systems or other related field. Five to ten years progressive management experience in Information Systems required. Experience with a multi-unit/integrated healthcare system preferred. Demonstrated successful leadership in planning, developing, and implementing management information processes, mechanisms, and systems is required. Excellent communication skills, leadership skills, negotiation skills, and motivational abilities are a must.

POSITION SUMMARY:

Responsible for <<XX>> Health Care System's Information Systems Division. This division includes Information Management, Health Information Management and Telecommunications for our multi-location/integrated healthcare system operating 24 hours a day, 365 days a year. This job description is congruent with the human and community development philosophy of the <<XX>>. The philosophy emphasizes responsibility for human life and the dignity and worth of every person. It also promotes the creation of caring communities in which the needs of those serving and being served are met. It is expected employees will perform their jobs in accordance with the philosophy.

ESSENTIAL FUNCTIONS:

1. Knows, understands, incorporates, and demonstrates the <<XX>>Health Care System(<<XX>>) Mission, Visions, Values, and Management Philosophy in leadership behaviors, practices, and decisions.
2. Monitors the health care delivery environment in order to anticipate any impact on information systems and communications networks to ensure appropriate utilization of information technology.
3. Examines new systems and develops strategies directed toward increased productivity by improving the work environment through systems and people consistent with the Mission, Vision, Values, and Management Philosophy of the <<XX>> system.
4. Establishes system-wide information management/technology standards and strategies for achieving integration and interoperability of information systems, technology architecture, and selection of software applications.
5. Maintains responsibility for the information system operations including the development and management of operating and capital budgets, policies, human resource utilization, mission effectiveness, and the overall performance of information technology within <<XX>> Health Care System.
6. Develops long-range plans and associated capital and expense budgets and monitors the achievement of these plans in order to ensure the successful performance of the organization.
7. Develops information system plans and programs to improve organization effectiveness and efficiency, ensuring that the information needs of <<XX>> Health Care System information technology staff are met.
8. Creates a seamless process to gather information regarding operational, human resources, financial, and clinical outcomes.
9. Maintains internal and external relationships with all system users and vendors.

10. Responsible for the installation of all new information systems and telecommunication systems for <<XX>> Health Care System.
11. Is a member of the Executive Team providing leadership to <<XX>> Health Care System.
12. Maintains the integrity and security of <<XX>> Health Care System's information systems, complying with all regulatory agencies and statutes.
13. Provides for professional growth and career opportunities for the Information System division staff.

OTHER FUNCTIONS:

1. All other duties as assigned.

APPROVED BY:

DEPARTMENT HEAD
DATE

PRESIDENT'S COUNCIL MEMBER
DATE

HUMAN RESOURCES DEPARTMENT
DATE**REVISION DATES:** _____**FOR HUMAN RESOURCES DEPT. USE ONLY:**_____ **EXEMPT**_____ **NONEXEMPT**

adds new users to the systems. Because they may also design and implement system security, database administrators often plan and coordinate security measures. With the volume of sensitive data growing rapidly, data integrity, backup systems, and database security have become increasingly important aspects of the job for database administrators (Department of Labor, Bureau of Labor Statistics, 2004).

The Network Administrator. As discussed in Part Three of this book, it is essential that the organization has an adequate network or network infrastructure to support all its clinical and administrative applications and also its general applications (such as e-mail, intranets, and the like). Networks come in many variations, so *network administrators* are needed to design, test, and evaluate systems such as local area networks

FIGURE 11.3. SAMPLE CMIO JOB DESCRIPTION.

JOB DESCRIPTION FOR CHIEF MEDICAL INFORMATION OFFICER

BACKGROUND

The position of Chief Medical Information Officer is a newly created position and reports to the Senior Vice President Information Services, CIO. This individual will lead the development and implementation of automated support for clinicians and clinical analysts through researching, recommending, and facilitating major and advanced clinical information system initiatives for the health care system.

In this role, the incumbent will provide reviews of medical informatics experiences and approaches, develop technical and application implementation strategies, manage implementation of advanced clinical information systems, assist in the development of strategic plans for clinical information systems, and provide project management for co-development relationships with the vendor community.

Information technology at THE HOSPITAL is becoming highly user driven. Governed by the Quality Council, a Clinical Informatics Steering Committee and subcommittees reporting to the Clinical Informatics Steering Committee will be formed to provide a user forum for input, coordination, and integration of information technology with THE HOSPITAL. The Director of Medical Informatics will chair, lead, and support the Clinical Informatics Steering Committee.

The following are ongoing responsibilities of the CHIEF MEDICAL INFORMATION OFFICER:

- Lead the implementation of a computerized patient record (CPR) system for the health care system (hospitals, clinics, physicians offices, ancillary and therapy units). This system should embody an information model focused on the diagnosis, treatment, and process data that will be required in future treatment and preventive care.

- Engage providers with varying roles including independent and employed physicians and clinicians, medical records professionals, and clinical analysts to contribute to the development and use of the CPR and analysis tools.

- Lead and support the Clinical Informatics Steering Committee which serves as the principal user governance forum to determine organizational priorities in this area.

- Stay attuned to the national effort to develop comprehensive, functional, and uniform medical records, and take an active role in areas where the national effort and health care system can mutually benefit.

- Be highly responsive to users' needs, including training, to ensure widespread acceptance and provider use of the clinical systems.

The following are expected accomplishments of the Chief Medical Information Officer for the first 12 to 24 months.

Gain a thorough understanding of the personality and culture of the organization and community; evaluate and refine the strategic information plan as it relates to clinical informatics.

Develop empathy and understanding of physician needs; build relationships with physicians to gain the support of physician leadership.

Together with a team leader evaluate the skills of the current clinical informatics team, identify needs and build a strong team by enhancing team members' skill base, motivating them and fostering a collaborative approach that values their contribution.

Design a model of the clinical database(s) to support the enterprise-wide CPR. The database(s) should support individual patient care and clinical studies across the full continuum of care.

Guided by the Quality Council, determine an approach and plan for the development and implementation of clinical systems that are components of a computerized patient record. The CPR will be designed to support clinicians in the care of patients throughout the network.

Select the products and vendors for the components of the initial phase of CPR implementation. Be on schedule, according to plan, with the implementations.

Implement physician network services, the transfer of clinical information between network sites, and the presentation of that information on a physician workstation.

The following are the desired credentials, skills, and personality characteristics of the ideal candidate (not listed in priority order):

The successful candidate will have the following profile:

A licensed physician with recent medical practice experience, graduate degree in medical informatics, and one year of work experience in medical informatics. In lieu of graduate training in medical informatics, a minimum of three years' work experience in medical informatics systems will be required.

A personable individual with excellent interpersonal and communication skills who can handle a diversity of personalities and interact effectively with people at all levels of the organization.

A strong leader with a mature sense of priorities and solid practical experience to implement the vision for the organization.

FIGURE 11.3. (continued)

An individual who is politically savvy, has a high tolerance for ambiguity, and can work successfully in a matrix management model.

A systems thinker with strong organizational skills who can pull all the pieces together and understand how to deliver ideals.

A strong manager who is adaptable and has a strong collaborative management style.

A creative thinker with high energy and enthusiasm.

A team player and consensus builder who promotes the concept of people working together versus individual performance.

A contemporary clinician who understands major trends in health care and managed care and has extensive knowledge of currently available point-of-care products and medical informatics development.

An individual with strong self-confidence who is assertive without being arrogant or ostentatious and who possesses confidence in heavy physician interaction.

(LANs), wide area networks (WANs), the Internet, intranets, and other data communications systems. Networks can range from a connection between two offices in the same building to globally distributed connectivity to voice mail and e-mail systems across a host of different health care organizations. Network administrators perform network modeling, analysis, and planning; they may also research related products and make hardware and software recommendations.

The Telecommunications Specialist. Working closely with the network administrator is the *telecommunications specialist*. These specialists manage the organization's telephone systems—for example, the central phone system, cellular telephone infrastructure, and nurse call systems. They often manage the communication network to be used by the organization in the event of a disaster. Because of the progressive convergence of voice networks and data networks, they may design voice and data communication systems, supervise the installation of those systems, and provide maintenance and other services to staff throughout the organization after the system is installed.

Other IT Staff. The growth of the Internet and the expansion of the World Wide Web have generated a variety of occupations related to the design, development, and maintenance of Web sites and their servers. For example, *Web masters* are responsible for all

technical aspects of a Web site, including performance issues such as speed of access, and for approving the site content. *Web developers* are responsible for day-to-day site design and creation. Often health care organizations contract with an outside IT company to provide Internet-development functions such as those performed by a Web developer.

The distinctions between the roles and functions of IT staff may seem a bit murky in practice. In one organization the systems analyst might do computer programming, advise on network specifications, and assist in database development. In another organization the systems analyst might have a clinical focus and work primarily with the end users in a particular unit, such as a laboratory, identifying needs, addressing problems, and providing ongoing training and support.

The specific qualifications, roles, and functions of the various IT staff members are generally determined by the pattern of IT development and use within the organization. For example, in a large academic medical center, the IT staff may be actively involved in designing in-house applications, and therefore the organization may employ teams of IT staff to work with faculty and clinicians in developing customized IT tools. This same level of IT expertise would be rare in an organization that relies primarily on IT applications purchased from the health care IT vendor community.

Furthermore, an organization might have an in-house IT services department, yet outsource a number of IT functions to be performed by staff outside the organization.

Staff Attributes

In addition to ensuring that it has the appropriate IT functions and IT roles (and that the individuals filling these roles are competent), the health care organization must ensure that the IT staff have certain attributes. These attributes are unlikely to arise spontaneously; they must often be managed into existence. An assessment of the IT function (as discussed later in this chapter) can highlight problems in this area and then lead to management steps designed to improve staff attributes.

High-performing IT staff have several general characteristics:

- *They execute well.* They deliver applications, infrastructure, and services that reflect a sound understanding of organization needs. These deliverables occur on time and on budget, so that those involved in the project give the project team high marks for professional comportment.
- *They are good consultants.* They advise organization members on the best approach to the application of IT given the organizational problem or opportunity. They advise when IT may be inappropriate or the least important component of the solution. This advice ranges from help desk support to systems analyses to new technology recommendations to advice on the suitability of IT for furthering an aspect of organization strategy.

- *They provide world-class support.* Information systems require daily care and feeding and problem identification and correction. This support needs to be exceptionally efficient and effective.
- *They stay current in their field of expertise.* They keep up to date on new techniques and technologies that may improve the ability of the organization to apply IT effectively.

Recruitment and Retention of IT Staff

In addition to ensuring that IT staff possess desired attributes, senior leadership may become involved in discussions centered on the attraction and retention of IT staff. Although the IT job market ebbs and flows, the market for talented and experienced IT staff is likely to be competitive for some time (Committee on Workforce Needs in Information Technology, 2001).

Recruitment and retention strategies involve making choices about what work factors and management practices will be changed and how they will be changed in order to improve the organization's ability to recruit and retain. Management may need to determine whether the focus will be on salaries or career development or physical surroundings or some combination of these factors.

For example, the IT managers at Partners HealthCare were asked to identify the factors that make an organization a great place to work and then to rate the Partners IT group on those factors, using letter grades. The factors identified by the managers included

- Salary and benefits
- Physical quality of the work setting, for example, well-maintained surroundings
- Caliber of IT management
- Amount of interesting work
- Importance of the organization's mission
- Opportunities for career growth
- Adequacy of communication about topics ranging from strategy to project status

The managers' grades for Partners IT on these factors are presented in Table 11.1. Using these scores, Partners IT leadership decided to focus on

- Establishing more thorough and better-defined career paths and development programs for all staff
- Improving training opportunities, ranging from brown bag lunches with invited speakers to technical training to supervisory training to leadership training
- Reviewing work environment factors such as parking, free amenities (such as soda), and office furniture

TABLE 11.1. MANAGERS' GRADES FOR WORK FACTORS.

	A	B	C	D	F
Compensation and benefits	1	14	12	3	
Work environment	4	17	4	3	2
Good management	6	13	8	3	
Interesting work	12	2			
Mission	17	12	1		
Career growth	4	19	5	2	
Communication		8	15	0	5
Status of organization	17	10	3		
TOTAL	61	95	48	11	7

- Improving communication through mechanisms such as sending a monthly e-mail from the CIO, videotaping staff meetings so they could be accessed through streaming media, and having regular dinners and lunches hosted by the CIO and deputy CIO

Taking steps such as these is important. Fundamentally, people work at organizations where the work is challenging and meaningful. They work at places where they like their coworkers and respect their leadership. They work at places where they are proud of the organization, its mission, and its successes.

Organizing IT Staff and Services

Now that we have introduced the various roles and functions found in the health care IT arena, we will examine how these roles and functions can be organized. Essentially, four factors influence the structure of the IT department:

- Definition and formation of major IT units
- Degree of IT centralization or decentralization
- Core IT competencies
- Departmental attributes

Definition and Formation of Major IT Units

There is no single right way to organize IT, and a department may iterate various organizational approaches in an effort to find the one that works best for it. (No approach

is free of limitations.) There are several overall approaches to structuring formal departments, and a department may employ several approaches simultaneously.

First, many IT departments organize their staff according to major job function or service areas. For example, a department might have a communications unit that sets up and manages local area networks and access to wide area networks, a research and development unit that keeps abreast of technology advances and experiments with new products, and a data administration unit that designs and maintains the organization's databases, data warehouses, and data management applications. Under this structure, staff members working in these various areas typically have both specialized and common skills, which they then apply to a wide range of systems or applications throughout the organization.

Second, the IT staff and services may be organized along product lines. That is, IT staff might work as project teams to develop, implement, maintain, and support a particular application or suite of applications. For example, there might be an applications unit comprising five to six major project teams. One team might support the administrative and billing systems, a second might support human and facility resources, and a third might cover clinical areas such as the laboratory, pharmacy, radiology, or nursing. Each team might combine IT staff and end users from the respective area. For example, a CPOE project team might include a systems analyst, a network administrator, a database manager, and key representatives from the clinical areas—medicine, nursing, laboratory, pharmacy, for example. This approach enables team members to work together closely, gain extensive knowledge about a particular application or suite of applications, and engage in holistic problem solving. In fact the IT staff may be physically located together near the user department.

Third, the IT staff may be organized according to critical organization processes. For example, there may be an IT team that manages and provides IT services to support the patient revenue cycle or patient access or medical services. This organization would enable the IT staff to understand all of the information systems issues associated with a cross-organization process and develop a comprehensive understanding of critical organization processes. This approach recognizes that patient care is based not on processes defined by organizational silos, for example, the laboratory or admitting, but rather on processes that cut across silos. Despite the conceptual appeal of this approach to IT organization, it is not common. Its rarity is due largely to the fact that most organizations are organized by departments and not cross-organization processes—for example, it is rare to see a vice president of patient access. In general it is not intelligent to have IT organized according to an approach that is radically different from the approach used by the organization overall.

Fourth, the IT department may support an organization that has multiple subsidiaries and divisions that may span a wide geography—an integrated delivery system (IDS), composed of multiple hospitals, for example. The form of the IT department in

an IDS is invariably matrixed. Kilbridge et al. (1998), in a study of IT departmental organization in integrated delivery systems, found three dimensions that defined this matrix. The *functional* dimension was devoted to IDS-wide infrastructure—for example, a communications network and enterprise master person index—and the support of IDS-wide consolidated functions—for example, finance. The geographical dimension was devoted to supporting distinct geographical sites or logically separate provider sites—for example, one of the IDS community hospitals. The cross-continuum process-oriented dimension might support acute care in general or a *carve out*, such as oncology services. Figure 11.4 depicts a two-dimensional structure based on function and geography. Figure 11.5 shows a two-dimensional structure based on function and process.

These four approaches are by no means the only way that one might approach organizing IT staff. The CIO, in conjunction with the organization’s executive team, should consider a wide range of options for organizing IT staff and resources. As part of this process the executive team should seek input from key constituents, examine the culture of the organization and the IT department, assess the long-term goals of the organization, and ultimately, employ a structure that facilitates IT staff efficiency

FIGURE 11.4. IT DEPARTMENT ORGANIZED BY FUNCTION AND GEOGRAPHY.

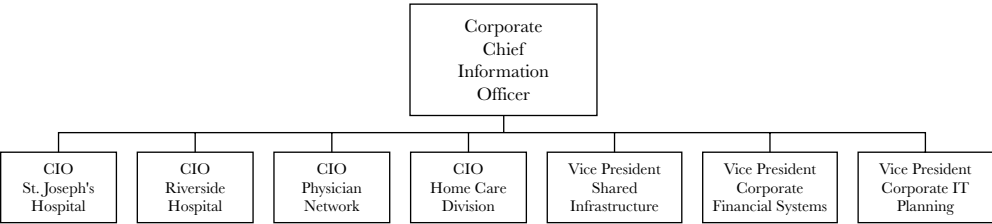
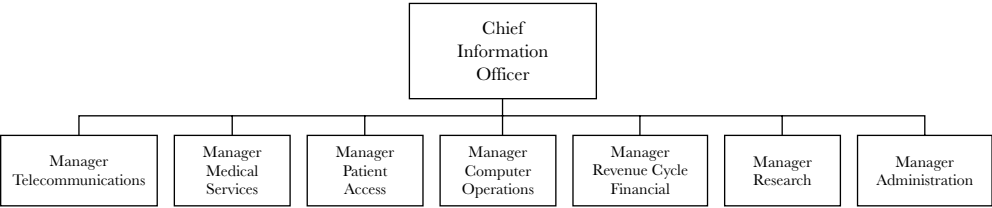


FIGURE 11.5. IT DEPARTMENT ORGANIZED BY FUNCTION AND PROCESS.



and effectiveness. The strategic questions in determining the structure of the IT organization are: Which approaches will be used? Do the IT groupings represent well-circumscribed clusters of like expertise or common goals? and, Is the resulting set of departments comprehensive in scope?

Degree of IT Centralization or Decentralization

A critical factor in determining the structure for the IT department is the degree of centralization of organization decision making. A health care organization might be a highly structured, vertical hierarchy where decisions are made by a few senior leaders. Conversely, an organization might delegate authority to the departmental level, or to the hospital level in an integrated delivery system, resulting in decentralized decision making.

There is no right level of centralization. Centralized organizations can be as effective as decentralized organizations. There are trade-offs. For example, centralized organizations are more likely to be able to effect uniformity of operations and to be more rational in their allocation of capital dollars, whereas decentralized organizations are more likely to be innovative. Moreover, an organization can be centralized in some areas—for example, the process for developing the budget—and decentralized in other areas—for example, developing marketing plans.

Ideally, the management and structure of IT will parallel that of the executive team's management philosophy; centralized management tends to want centralized control over IT whereas decentralized management is more likely to be comfortable with local responsiveness of IT.

One approach is not necessarily better than the other; they both have advantages and trade-offs. Some of the advantages to centralizing IT services are (Oz, 2004)

- *Enforcement of hardware and software standards.* In a centralized structure the organization typically develops software and hardware standards, which can lead to cost savings, facilitate the exchange of data among systems, make installations easier, and promote sharing of applications.
- *Efficient administration of resources.* Centralizing the administration of contracts and licenses and inventories of hardware and software can lead to greater efficiency.
- *Better staffing.* Because it results in a pool of IT staff from which to choose, the centralized approach may be able to identify and assign the most appropriate individuals to a particular project.
- *Easier training.* In a centralized department, staff can specialize in certain areas (hardware, software, networks) and do not need to be jacks of all trades.
- *Effective planning of shared systems.* A centralized IT services unit typically sees the big picture and can facilitate the deployment of systems that are to be used by all units of a health care system or across organization boundaries.

- *Easier strategic IT planning.* A strategic IT plan should be well aligned with the overall strategic plan of the organization. This alignment may be easier when IT management is centralized.
- *Tighter control by senior management.* A centralized approach to managing IT services permits senior management to maintain tighter control on the IT budget and resources.

Despite the advantages of a more centralized approach to managing IT services, many health care organizations have moved in recent years to a relatively decentralized structure. Some of the advantages to a decentralized structure are (Oz, 2004)

- *Better fit of IT to business needs.* The individual IT units are familiar with their business unit's or department's needs and can develop or select systems that fit those needs more closely.
- *Quick response time.* The individual IT units are typically better equipped to respond promptly to requests or can arrange IT projects to fit the priorities of their business unit or department.
- *Encouragement of end-user development of applications.* In a decentralized IT services structure, end users are often encouraged to develop their own small applications to increase productivity.
- *Innovative use of information systems.* Given that IT staff are closer in proximity to users and know their needs, the decentralized structure may have a better chance of implementing innovative systems.

Most IT services in a health care organization are not fully centralized or decentralized but a combination of the two. For example, training and support for applications may be decentralized, with other IT functions such as application development, network support, and database management being managed centrally. The size, complexity, and culture of the health care organization might also determine the degree to which IT services should be managed centrally. For example, in an ambulatory care clinic with three sites that are fairly autonomous it may be appropriate to divide IT services into three functional units, each dedicated to a specific clinic. In a larger, more complex organization, such as an integrated delivery network (with multiple hospitals, outpatient clinics, and physician practices), it may be appropriate to form a centralized IT services unit that is responsible for specific IT areas such as systems planning and integration, network administration, and telecommunications, with all other functions being managed at the individual facility level (DeLuca & Enmark, 2002).

Core IT Competencies

Organizations should identify a small number of areas that constitute core IT capabilities and competencies. These are areas where getting an A+ from the “customers”

matters. For example, an organization focused on transforming its care processes would want to ensure A+ competency in this area and would perhaps settle for B— competency in its supply chain operations. An organization dedicated to being very efficient would want A+ competency in areas such as supplier management and productivity improvement and would perhaps settle for a B— in delivering superb customer service.

This definition of core competencies has a bearing on the form of the IT organization. If A+ competency is desired in care transformation, the IT department should be organized into functions that specialize in supporting care transformation—for example, a clinical information systems implementation group and a care reengineering group.

Partners HealthCare, for example, defined three areas of core capabilities: base support and services, care improvement, and technical infrastructure.

Base Support and Services. This category of core capabilities at Partners HealthCare included two subcategories:

- Frontline support: for example, PC problem resolution
- Project management skills

The choice of these areas of emphasis resulted in many management actions and steps—for example, the selection of criteria to be used during annual performance reviews. The emphasis on frontline support also led to the creation of an IT function responsible for all frontline support activities, including the help desk, deployments of workstations, training, and user account management. The emphasis on project management led to the creation of a project management office to assist in monitoring the status of all projects and a “project center of excellence” to offer training on project management and established project management standards.

Care Improvement. Central to the Partners agenda was the application of IT to improve the process of care. One consequence was to establish, as a core IT capability, the set of skills and people necessary to innovatively apply IT to medical care improvement. An applied medical informatics function was established to oversee a research and development agenda. Staff skilled in clinical information systems application development were hired. A group of experienced clinical information system implementers was established. An IT unit of health services researchers was formed to analyze deficiencies in care processes, identify IT solutions that would reduce or eliminate these deficiencies, and assess the impact of clinical information systems on care improvement. Organizational units possessing unique technical and clinical knowledge in radiology imaging systems and telemedicine were also created.

Technical Infrastructure. Recognizing the critical role played by having a well-conceived, well-executed, and well-supported technical architecture, infrastructure architecture and design continued to serve as a core competency. A technology strategy function was created, and the role of chief technology officer was created. Significant attention was paid to ensuring that extremely talented architectural and engineering staff were hired along with staff with terrific support skills.

Departmental Attributes

IT departments, like people, have characteristics or attributes. They may be agile or ossified. They may be risk tolerant or risk averse. These characteristics can be stated, and strategies to achieve desired characteristics can be defined and implemented. To illustrate, this section will briefly discuss two characteristics—agility and innovativeness—and discuss how they might affect the organization of IT functions. These two are representative and are generally viewed as desirable.

There are many steps that an organization can take to increase its overall agility and also that of the IT department. For example, it is likely to try to *chunk* its initiatives so that there are multiple points at which a project can be reasonably stopped and yet still deliver value. Thus the rollout of a computerized medical record might call for implementation at ten clinics per year but could be stopped temporarily at four clinics and still deliver value to those four. Chunking allows an organization and its departments to quickly shift emphasis from one project to another.

An agile IT department will have the ability to form and disband teams quickly (perhaps every three months) as staff move from project to project. This requires that organizational structures and reporting relationships be flexible so staff can move rapidly between projects. It also means that during a project, the project manager is (temporarily anyway) the boss of the project team members. The team members might report to someone else according to the organization chart, but their real boss at this time is the project manager. Because team members might move rapidly from project to project, they might have several bosses during the course of a year. And a person might be the boss on one project and the subordinate on another project. Agile organizations and departments are organized less around functions and more around projects. The IT structure must accommodate continuous project team formation, and project managers must have significant authority.

An organization or department that wants to be innovative might take steps such as implementing reward systems that encourage new ideas and successful implementation of innovative applications and punishment systems that are loath to punish those involved in experiments that failed. The innovative IT department might create dedicated research and development groups. It might form teams composed of IT staff

and vendor staff in an effort to cross-fertilize each staff with the ideas of the other. It might also permit staff to take sabbaticals or accept internal internships with other departments in the organization in an effort to expand IT members' awareness of organization operations, cultures, and issues.

In-House Versus Outsourced IT Services

For the past two decades, health care organizations have generally provided IT services in-house. By *in-house* we mean that the organization hired its own IT staff and formed its own IT department. In recent years, however, health care organizations have shown a growing interest in outsourcing part or all of their IT services. Outsourcing IT means that an organization asks a third party to provide the IT staff and be responsible for the management of IT. Results from a recent Healthcare Information and Management Systems Society (HIMSS) survey indicate that 70 percent of participating CIOs currently outsource at least one IT function, with the three most common functions being Web-site development and maintenance (32 percent), applications development (19 percent), and application service provider-type arrangements (16 percent) (HIMSS, 2003a).

The reasons for outsourcing IT functions are varied. Some health care organizations may simply not have staff with the skills, time, or resources needed to take on new IT projects or provide sufficient IT service. Others may choose to outsource certain IT functions, such as help desk services or Web-site development, so that internal IT staff can focus their time on implementing or supporting applications central to the organization's strategic goals. Still other organizations contract with an application service provider (ASP) to run system applications, manage the data, and provide technical support. Outsourcing IT may enable organizations to better control costs. Because a contract is typically established for a defined scope of work to be done over a specific period of time, the IT function becomes a line item that can be more effectively budgeted over time. This does not mean, however, that outsourcing IT services is necessarily more cost effective than providing IT services in-house. At times new organizational leadership finds an IT function that is in disastrous condition. After years of mismanagement, applications may function poorly, the infrastructure may be unstable, and the IT staff may be demoralized. An outsourcing company may be brought in as a form of rescue mission.

A number of factors come into play and should be considered when evaluating whether outsourcing part or all of IT services is in the best interest of the organization. The questions asked should include the following:

- Does our organization have IT staff with the knowledge and skills needed to provide necessary services? Effectively manage projects? Adequately support current applications and infrastructure?

- How easy or difficult is it to recruit and retain qualified IT staff?
- What are our organization's major IT priorities? How equipped is our organization to address these priorities? Do we have the right mix of skills, time, and resources?
- What benefits might be realized from outsourcing this IT function? What are the risks? Do the benefits outweigh the risks?
- What parts, if any, of the IT department does it make the most sense to outsource?
- If we opt to outsource IT services, whom do we want to do business with? How will we monitor and evaluate IT performance and service? What provisions will we make in the contract with the outsourcing company to ensure timeliness and quality of service? How will the terms of the contract be monitored?

It is important to evaluate the cost and effectiveness of the IT function and services, whether they are performed by in-house staff or outsourced. There are pros and cons to each, and the organization must make its decision based upon its strategy goals and priorities. There is no silver bullet or one solution for all.

Evaluating the Effectiveness of the IT Function

Whether IT services are provided by in-house staff or are outsourced, it is important to evaluate IT performance. Is the function efficient? Does it deliver good service? Is it on top of new developments in its field? Does the function have a strong management team?

At times, health care executives become worried about the performance of an IT function. Other organizations have IT functions that seem to accomplish more or spend less. Management and physicians frequently express dissatisfaction with IT; nothing is getting done, it costs too much, or it takes too long to get a new PC. Many factors may result in user dissatisfaction: poor expectation setting, unclear priorities, limited funding, or inadequate IT leadership. An assessment of IT services can help management understand the nature of the problems and identify opportunities for improvement.

One desirable approach to assessing IT services is to use outside consultants. Consultants can bring a level of objectivity to the assessment process that is difficult to achieve internally. They can also share their experiences from having worked with a variety of different health care organizations and having observed different ways of handling some of the same issues or problems.

Whether the assessment is done by internal staff or by consultants, several key areas should be addressed:

- Governance
- Budget development and resource allocation

- System acquisition
- System implementation
- IT service levels

Governance

How effective is the governance structure? To what degree are IT strategies well aligned with the organization's overall strategic goals? Is the CIO actively involved in strategy discussions? Does senior leadership discuss IT agenda items on a regular basis? We will discuss governance in Chapter Thirteen.

Budget Development and Resource Allocation

The IT budget is often compared to the IT budgets of comparable health care organizations. The question behind a budget benchmark is, "Are we spending too much or too little on IT?" Budget benchmarks are expressed in terms of the IT operating budget as a percentage of the overall organization's operating budget. These numbers are calculated with and without depreciation. "Average" percentages are 2.5 percent (IT operating budget/overall operating budget) and 4.6 percent (with depreciation added to the numerator and denominator) (Cruz, 2003).

These budget benchmarks are useful and in some sense required because most boards of directors expect to see them. Management has to be careful in interpreting the results, however. These percentages do not necessarily reflect the quality of IT services or the extent and size of the organization's application base or infrastructure. Hence one can find a poorly performing IT group that has implemented little employing the same percentage of the organization's budgetary resources as a world-class IT group that has implemented a stunning array of applications.

A high percentage—for example, 4.5 percent (without depreciation)—does not per se mean that the organization is spending too much and should reduce its IT budget. The organization may have decided to ramp up its IT investments in order to achieve certain strategic objectives. A low percentage—for example, 1 percent (without depreciation)—does not per se mean that underinvestment is occurring and the IT budget should be significantly increased. The organization may be very efficient, or it may have decided that given its strategies its investments should be made elsewhere.

System Acquisition

How effective are system acquisitions? How long did they take? What process was used to select the systems? We discussed system acquisition in Chapter Six.

System Implementation

Are new applications delivered on time, within budget, and according to specification? Do the participants in the implementation speak fondly of the professionalism of the IT staff or do they view IT staff as forms of demonic creatures? We discussed system implementation in Chapter Seven.

IT Service Levels

IT staff deliver service every day—for example, they manage system performance, respond to help desk calls, and manage projects. The quality of these services can be measured. An assessment of the IT function invariably reviews these measures and the management processes in place to monitor and improve IT services. IT users in the organization are interested in measures such as these:

- *Infrastructure.* Are the information systems reliable, that is, do they rarely “go down”? Are response times fast?
- *Day-to-day support.* Does the help desk quickly, patiently, and effectively resolve my problems? If I ask for a new workstation, does it arrive in a reasonable period of time?
- *Consultation.* Are the IT folks good at helping me think through my IT needs? Are they realistic in helping me to understand what the technology will and will not do?

An organization faces a challenge in defining what level of IT service it would like and also how much it is willing to pay for IT services. All of us would love to have system analysts with world-class consulting skills, but we may not be able to afford their salaries. Similarly, all of us would love to have systems that never go down and are as fast as greased lightning, but we might not be willing to pay the cost of engineering very, very high reliability and blazing speed. The IT service conversation attempts to establish formal and measurable levels of service and the cost of providing that service. The organization seeks an informed conversation about the desirability and the cost of improving the service or the possibility of degrading the service in an effort to reduce costs.

In general it can be very difficult to measure the quality and consequences of consultative services. This makes it difficult to understand whether it is worth investing to improve the service other than at the service extremes. For example, it can be clear that you need to fire a very ineffective systems analyst and that you need to treat your all-star analyst very well. But it may not be clear whether paying \$10,000 extra for an IT staff member is worth it or not.

Formal, measurable service levels can be established for many infrastructure attributes and day-to-day support. Moreover, industry benchmarks exist for these measures. Infrastructure service metrics may include

- Reliability: for example, the percentage of time that systems have unscheduled downtime
- Response time: for example, how quickly an application moves from one screen to the next
- Resiliency: for example, how quickly a system can recover after it goes down
- Software bugs: for example, the number of bugs detected in an application per line of program code or hour of use

Day-to-day support service metrics may include

- The percentage of help desk calls that are resolved within twenty-four hours
- The percentage of help desk calls that are not resolved after five days
- The percentage of help desk call that are repeat calls: that is, the problem was not resolved the first time
- The time elapsed between ordering a personal computer and its installation

It is important that the management team define the desired level of IT service. For example, is the goal to achieve an uptime of 99.9 percent, or do we want to have 90 percent of help desk calls closed within twenty-four hours? If the service levels are deemed to be inadequate, a discussion can be held with IT managers to identify the costs of achieving a higher level of service. Additional staff may be needed at the help desk, or the organization may need to develop a redundant network to improve resiliency. Conversely, if the organization needs to reduce IT costs, the management team may need to examine the service consequences of reducing the number of help desk staff.

The assessment of the IT function centers on the degree to which service levels are being met and whether effective discussions have been held with organization leadership about the desired level of service and costs of achieving that level. Following are two sets of suggested items to examine in an assessment. Exhibit 11.1 is a sample survey used by an IT services department to assess user satisfaction.

Perspective: Assessing the IT Function

John Glaser suggests the following as a crude, quick way of assessing the IT function:

- Ask three members of the management team to identify the major IT initiatives for the next year. Inconsistent answers or blank stares indicate a failure in the IT planning process.

- Review the expectations that were set for the last two systems you purchased. Ask for an assessment of the extent to which the goals were met and whether the implementations were on time and on budget.
- Ask for information to support two upcoming strategic or management decisions. See whether, how quickly, and at what costs the requests can be satisfied.
- Ask your CIO for his or her assessment of the role a new information technology might play in the organization. (An IT article in a health care management publication may provide an idea about the IT technology to suggest.) Did you understand the answer? Does the response seem thoughtful?
- Ask the CIO how your level of IT expenditures compares with the IT expenditures of comparable organizations. Although one has to be careful of viewing expenditure percentage data as a guide to a specific organization's decisions, the fact that such data are known means that organizations are worrying about their IT function costs and are comparing these costs to others' costs.
- Ask the help desk staff if they can tell you how many trouble calls the help desk received last month, the average time to correct the problem, and the number of repeat visits. A lack of such data indicates an orientation that still struggles to spell the word *service*.

Answers to these questions provide an indication, clearly rough, of how well the IT function is being run and, to a degree, whether the aggregate IT investment is providing value. All these questions come from common sense, management beliefs about what is involved in running an organization well, and tests of IT domain knowledge.

Glaser, 1991

Perspective: Managing Core IT Processes

Ritu Agarwal and Vallabh Sambamurthy have identified eight core IT processes that must be managed well for an IT department to be effective:

1. *Human capital management* involves the development of IT staff skills and the attraction and retention of IT talent.
2. *Platform management* is a series of activities that designs the IT architecture and constructs and manages the resulting infrastructure.
3. *Relationship management* centers on developing and maintaining relationships between the IT function and the rest of the organization and on partnerships with IT vendors.
4. *Strategic planning* links the IT agenda and plans to the organization's strategy and plans.
5. *Financial management* encompasses a wide range of management processes—developing the IT budget, defining the business case for IT investments, and benchmarking IT costs.

EXHIBIT 11.1. SAMPLE USER SATISFACTION SURVEY.



CUSTOMER SERVICE SURVEY

University Administration and the Center for Computing and Information Technology (CCIT) are reaffirming their commitment to continuous improvement of their services by asking for your feedback on CCIT's quality of service to you. The questions are intended to give us input on the department's strengths and weaknesses and get a feel as to what you, our customers, would like to see. Please be frank and candid in your answers. Only with your help can we improve the services CCIT provides to you!

If you would prefer, you can complete this survey on-line at <http://www.musc.edu/ccit/>.

Thank you in advance for your participation!

Please, tell us about yourself . . .

You are: (circle one) Faculty Staff Information Technology Coordinator Student Resident Temp

If "staff" or "temp," where do you work?

College Ambulatory Care / Medical Center/UMA Finance and Administration University Support (for example, Enrollment Services, Library)

Does your department have a computer support resource (for example, ITC)? Yes No Don't Know

Which CCIT-supported systems do you use? (circle all used routinely)

General

Audix (voice mail) CentreVu (CMS) Internet services PPP server Telephone

Information References

Auget Catalyst "Tips" CCIT web page Keane newsletter PacketXpress

Educational/Research Systems

American Fundware CDMIS Faculty Profile System Grants Accounting GCG, Sybyl Homeroom
MUSCLS Netscape Calendar Ovid SPSS (UNIX) Usenet News WWW Server

Clinical Systems

AeroMed ANSOS AutoTrack Burn Unit MR Cerner Pathology Coding (3M)
DeMedici Downtime MPI DS Plus EPS ESI/Nova GI Trac / GI Image

HARP IDXRad Infection Control Keane / PatcomPlus LANVision Med Staff
MediLinks MediScribe Meduline/Centramax MRS / Tumor Reg. MSMeds/Megasource MSDS
MUSCHealth.com MUSE NucMed Pharmacy Oacis / Passport Odyssey Oversite
PACS PAID QS1 OP Pharmacy RenalStar SMS Summit
SurgiServer Trendstar Velos VingMed/EchoPac

Administrative and Financial Systems

Colleague/Datatel Effort Reporting HeRMIT Parking Svcs SmartStream STAR/Kronos

Workstation Support (circle your configuration)

ClinLAN Macintosh Win 95/'98/NT/2000 Linux / UNIX FinLAN / Metaframe / Citrix

Now, what do you think about us . . .

Help Desk Staff	Very satisfied	Somewhat satisfied	Neutral	Somewhat dissatisfied	Very dissatisfied
1. Requests are clearly understood	5	4	3	2	1
2. Troubleshooting skills are adequate	5	4	3	2	1
3. If not able to resolve, are able to identify right resource	5	4	3	2	1
4. Professional, friendly, diplomatic	5	4	3	2	1
5. Understands needs and priorities	5	4	3	2	1
6. Treats you with respect and consideration	5	4	3	2	1

Systems Support Staff

1. Responsive to problems/requests	5	4	3	2	1
2. Professional, friendly, diplomatic	5	4	3	2	1
3. Understands needs and priorities	5	4	3	2	1
4. Treats you with respect and consideration	5	4	3	2	1
5. Communicates well	5	4	3	2	1
6. Quality of work is high	5	4	3	2	1
7. Positive attitude	5	4	3	2	1
8. Plans/manages projects well	5	4	3	2	1

Workstation Support Staff

1. Responsive to problems/requests	5	4	3	2	1
2. Professional, friendly, diplomatic	5	4	3	2	1
3. Understands needs and priorities	5	4	3	2	1
4. Treats you with respect and consideration	5	4	3	2	1
5. Communicates well	5	4	3	2	1
6. Quality of work is high	5	4	3	2	1
7. Positive attitude	5	4	3	2	1
8. Plans/manages projects well	5	4	3	2	1

Do you have additional comments about your experiences with our staff?

Overall, how satisfied are you with CCIT? very satisfied satisfied neutral not satisfied very dissatisfied

Would you like to be interviewed? For “yes,” please note your name and MUSC extension:

Thank you again for your time and assistance!

6. *Value innovation* involves identifying new ways for IT to improve business operations and ensuring that IT investments deliver value.
7. *Solutions delivery* includes the selection, development, and implementation of applications and infrastructure.
8. *Services provisioning* centers on the day-to-day support of applications and infrastructure: for example, the help desk, workstation deployments, and user training.

Agarwal and Sambamurthy, 2002

Summary

It is critical that health care organizations have access to appropriate IT staff and resources to support their health care information systems and system users. IT staff perform several common functions and have several common roles. In large organizations, the IT department often has a management team comprising the chief information officer, chief technology officer, chief security officer, and chief medical informatics officer, who provide leadership to ensure that the organization fulfills its IT strategies and goals. Having a CIO with strong leadership skills, vision, and experience is critical to the organization in achieving its strategic IT goals. Working with the CIO and IT management team, one will often find a team of professional and technical staff including system analysts, computer programmers, network administrators, database administrators, and web designers and support personnel. Each brings a unique set of knowledge and skills to support the IT operations of the health care organization.

The organizational structure of the IT department is influenced by several factors: definition of major units, level of centralization, core IT competencies, and desired attributes of the IT department.

IT services may be provided by in-house staff or outsourced to an outside vendor or company. Many factors come into play in deciding if and when to outsource all or part of the IT services. Availability of staff, time constraints, financial resources, and the executive management team's view of IT may determine the appropriateness of outsourcing.

Whether IT services are provided in-house or outsourced, it is important for the management team to assess the efficiency and effectiveness of IT services. The governance structure, how the IT resources are allocated, the track record of system acquisitions and system implementations, and user satisfaction with current IT service levels are some of the key elements that should be examined in any assessment. Consultants may be employed to conduct the assessment and offer the organization an outsider's objective view.

Chapter Eleven: Learning Activities

1. Visit an IT department in a health care facility in your community, and interview the CIO or department director. Examine the IT department's organizational structure. What functions or services does the IT department provide? How centralized are IT services within the organization? Does the organization employ a CMIO, CSO, or CTO? If so, what are each person's job qualifications and responsibilities?
2. Find an article in the literature that outlines either the advantages or disadvantages, or both, of outsourcing IT. Discuss the findings with your classmates. What have others learned about outsourcing that may be important to your organization?
3. Plan and organize a panel discussion with CIOs from local health care facilities. Find out what some of their greatest challenges are and what a typical day is like for them.
4. Assume that your organization is concerned about employee satisfaction with IT services. How might the organization assess employee satisfaction? What methods and tools might be used? How would you use these methods and tools?



CHAPTER TWELVE

IT ALIGNMENT AND STRATEGIC PLANNING

Information technology (IT) investments serve to advance organizational performance. These investments should enable the organization to reduce costs, improve service, enhance the quality of care, and in general, achieve its strategic objectives. The goal of IT alignment and strategic planning is to ensure a strong and clear relationship between IT investment decisions and the health care organization's overall strategies, goals, and objectives. For example, an organization's decision to invest in a new claims adjudication system should be the clear result of a goal of improving the effectiveness of its claims processing process. An organization's decision to implement a computerized provider order entry system should reflect an organization strategy of improving patient care.

Developing a sound alignment can be very important for one simple reason; if you define the IT agenda incorrectly or even partially correctly, you run the risk that significant organizational resources will be misdirected; the resources will not be put to furthering strategically important areas. This risk has nothing to do with how well you execute the IT direction you choose. Being on time, on budget, and on specification is of little value to the organization if it is doing the wrong thing!

The IT alignment and strategic-planning process has several broad objectives:

- Ensure that IT plans and activities are well linked to the plans and activities of the organization. In other words, the IT needs of each aspect of organization strategy are clear, and the overall portfolio of IT plans and activities can be mapped to organization strategies and operational needs.

- Ensure that the alignment is comprehensive. In other words, ensure that Each aspect of strategy has been addressed from an IT perspective, recognizing that not all aspects have an IT component and not all IT components will be funded.
The non-IT organizational initiatives have been addressed, such as any process reengineering needed to ensure maximum leverage of the IT initiative.
The organization has not missed a strategic IT opportunity—for example, one that might result from new technologies.
- Develop a tactical plan that details approved project descriptions, time tables, budgets, staffing plans, and plan risk factors.
- Create a communication tool that can inform the organization of the IT initiatives that will be undertaken and those that will not.
- Establish a political process that helps to ensure that the IT plan has sufficient organizational support.

At the end of the alignment and strategic-planning process an organization should have an outline that at a high level resembles Table 12.1. With this outline the leadership can see the IT investments needed to advance each of the organization's strategies. For example, the goal of improving the quality of patient care may lead the organization to invest in databases to measure and report quality, computerized provider order entry (CPOE), and the electronic medical record (EMR).

Despite the simplicity implied by Table 12.1, the development of well-aligned IT strategies has been notoriously difficult for many years, and there appears to be no reason that crafting this alignment will become significantly easier over time.

This chapter discusses the challenges of and approaches to IT alignment and strategic planning. We will cover

- An overview of strategy
- The areas requiring IT strategy
- Vectors for arriving at IT strategy
- The IT asset and governing concepts
- A normative approach to developing alignment and IT strategy
- The challenges of IT strategy and alignment
- Information technology as a competitive advantage

Overview of Strategy

The strategy of an organization has two major components (Henderson & Venkatraman, 1993): formulation and implementation.

TABLE 12.1. IT SUPPORT OF ORGANIZATION GOALS.

Goal	IS Initiatives
Research and education	• Research patient data registry • Genetics and genomics platform • Grants management
Patient care: quality improvement	• Quality measurement databases • Order entry • Electronic medical record
Patient care: sharing data across the system	• Enterprise master person index • Clinical data repository • Common infrastructure
Patient care: nonacute care services	• Nursing documentation • Transition of care application
Financial stability	• Revenue enhancements • PeopleSoft • Cost accounting

Formulation

Formulation of strategy involves making decisions about the mission and goals of the organization and the activities and initiatives that it will undertake to achieve that mission and those goals. Formulation may involve, for example, determining that

- Our mission is to provide high-quality medical care.
- We have a goal of reducing the cost of care while at least preserving the quality of that care.
- One of our greatest leverage points lies in reducing inappropriate and unnecessary care.
- To achieve this goal we will place emphasis on, for example, reducing the number of inappropriate radiology procedures.
- We will carry out initiatives that enable us to intervene at the time of procedure ordering if we need to suggest a more cost-effective modality.

The organization's members can imagine other goals directed to achieving the same mission. For each goal, they can envision multiple leverage points, and for each

leverage point they may see multiple initiatives. An inverted tree that cascades from the mission to a series of initiatives will emerge.

Formulation initiatives involve understanding competing ideas and choosing between them. In the example just given, leadership could have arrived at a different set of goals and initiatives. It could have decided to improve quality with less emphasis on care costs. It could have decided to focus on reducing the cost per procedure. It could have decided to produce retrospective reports, by provider, of radiology utilization and to use this feedback to manage behavioral change rather than deciding to intervene at the time of ordering.

IT strategy also needs formulation. For example, in keeping with an IT mission to use the technology to support the improvement of the quality of care, we may have a goal to integrate clinical application systems. To achieve this goal, we may decide to

- Provide a common way to access all systems (single sign on).
- Interface existing heterogeneous application systems.
- Require that all applications use a common database.
- Implement a common suite of clinical applications from one vendor.

Implementation

Implementation involves making decisions about how the organization structures itself, acquires skills, establishes capabilities, and alters processes in order to achieve the goals and carry out the activities that have been defined during formulation. For example, if we have decided to reduce care costs by reducing inappropriate procedure use, we may need to implement

- An organizational unit of providers with health service research training to analyze care practices and identify deficiencies
- A steering committee of clinical leadership to guide these efforts and provide political support
- A CPOE system to provide real-time feedback on order appropriateness
- Data warehouse technologies to support the analyses of utilization

Returning to the clinical applications integration example, we may, on the one hand, determine that we need to acquire interface engine technology, adopt HL7 standards, and form an IT function that manages the technology and interfaces applications. Or, on the other hand, we may decide we need to engage external consulting assistance for selection of a clinical application suite and that we need to hire a group to implement the suite.

The implementation component of strategy development is not the development of project plans and budgets. Rather it is the identification of those capabilities, capacities, and competencies that the organization will need if it is to carry out the results of the formulation component of strategy.

Areas Requiring IT Strategy

IT strategy is very important in these three major areas (which are discussed further in subsequent sections):

- *The development of the application agenda.* This agenda constitutes an inventory of desired applications or major improvements to existing applications. Table 12.1 presented an example of such an agenda.
- *Initiatives designed to improve the IT asset.* An organization's IT applications, infrastructure, data, staff and department, and governance are its *IT asset*. Initiatives can be designed to add major capabilities to this asset—the ability to access the organization's applications around the globe, for example. Or initiatives might aim to enhance characteristics of the asset—to make the IT organization more agile, for example.
- *Concepts that govern the approach to a class of initiatives and applications.* The notion of *governing concepts* can be difficult to get your mind around. However, it is essential to do so. Governing concepts define how an organization “thinks about” or “views” many different things. Some governing concepts will concern IT applications or the IT function. For example, does the organization want to be on the cutting edge of IT, or would it prefer to be more conservative, and why? Are Internet technologies viewed as tools that will enable organization transformation or are they seen as normal, incremental improvements in technology? Is the electronic medical record system viewed as primarily solving problems associated with the accessibility of the patient record or is it seen primarily as a means to improve disease management? Is it considered preferable to buy IT systems or build them?

Vectors for Arriving at IT Strategy

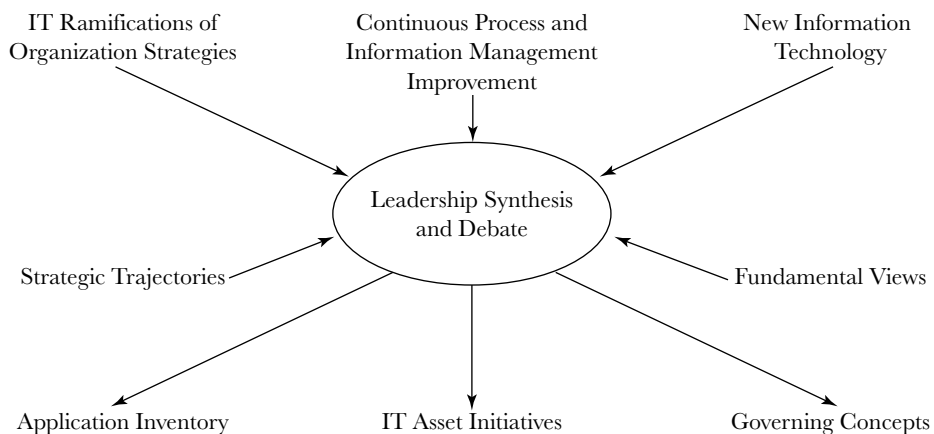
In many ways the content of Table 12.1 is deceiving. The table presents a tidy, orderly linkage between the IT agenda and the strategies of the organization. One might assume that this linkage is established through a linear, rational, and straightforward series of steps. But the process of arriving at a series of connections like those in Table 12.1 is complex, iterative, and at times driven by politics and instincts.

There are five major *vectors* an organization may follow to arrive at IT strategy. IT strategy may be

1. Based on organization strategies
2. Based on continuous improvement of core processes and information management
3. Based on examination of the role of new information technologies
4. Based on assessment of strategic trajectories
5. Based on fundamental views about competition or the nature of organizations

By a *vector* we mean the choice of perspectives and approaches through which an organization determines its IT investment decisions. For example, the first vector (derived from organization strategies) involves answering a question such as this: Given our strategy of improving patient safety, what IT applications will we need? However, the third vector (determined by examining the role of new information technologies) involves answering a question such as this: There is a great deal of discussion about wireless technologies. What types of applications would wireless enable us to perform and would these applications be important to us? Figure 12.1 illustrates the convergence of these five vectors into a series of iterative leadership discussions and debates. These debates lead to an IT agenda composed of an application inventory, IT asset initiatives, and governing concepts.

FIGURE 12.1. VECTORS FOR ARRIVING AT IT STRATEGY.



IT Strategies Based on Organization Strategies

The first vector involves deriving the IT agenda directly from the organization's goals and plans. For example, an organization may decide that it intends to become the low-cost provider of care. It may decide to achieve this goal through the implementation of disease management programs, the reengineering of inpatient care, and the reduction of unit costs for certain tests and procedures that it believes are inordinately expensive.

The IT strategy development then centers on answering questions such as these: How do we apply IT to support disease management? The answers might involve Web-based publication of disease management protocols for use by providers, data warehouse technology to assess the conformance of care practice to the protocols, provider documentation systems based on disease guidelines, and CPOE systems that employ the disease guidelines to guide ordering decisions. An organization may choose all or some of these responses and develop various sequences of implementation. Nonetheless, it has developed an answer to the question of how to apply IT in the support of disease management. The IT plan would define the application systems and resources—for example, staff and budgets—needed to support the goals.

Most of the time the linkage between organization strategy and IT strategy involves developing the IT ramifications of organizational initiatives such as adding or changing services and products, growing market share, or reducing costs. At times, however, an organization may decide that it needs to change or add to its core characteristics or culture. The organization may decide that it needs its staff to be more care quality or service-delivery or bottom-line oriented. It may decide that it needs to decentralize decision making or to recentralize decision making. It may decide to improve its ability to manage knowledge, or it may not. These characteristics, and there are many others, can point to initiatives for IT.

In the cases where characteristics are to be changed, IT strategies must be developed that answer questions like this: What is our basic approach to supporting a decentralized decision-making structure? The organization might answer this question by permitting decentralized choices of applications as long as those applications meet certain standards—for example, run on a common infrastructure or support a common database standard. It might answer the question of how IT supports an emphasis on knowledge management by developing an intranet service that provides access to preferred treatment guidelines.

IT Strategies Based on Continuous Improvement of Core Processes and Information Management

All organizations have a small number of core processes and information management tasks that are essential for the effective and efficient functioning of the organization. For

a hospital these processes might include ensuring patient access to care, ordering tests and procedures, and managing the revenue cycle. For a restaurant these processes might include menu design, food preparation, and dining room service. For a managed care organization, information management needs might point to a requirement to understand the costs of care or the degree to which care practices vary by physician.

Using the vector of continuous improvement of core processes and information management to determine IT strategies involves defining the organization's core processes and information management needs. The organization measures the performance of core processes and uses the resulting data to develop plans to improve its performance. The organization defines core information needs, identifies the gap between the current status and its needs, and develops plans to close those gaps. These plans will often point to an IT agenda.

This vector may be a result of a strategy discussion but not always. An organization may make ongoing efforts to improve processes regardless of the specifics of its strategic plan. For example, every year it may set initiatives designed to reduce costs or improve services.

Table 12.2 illustrates a process orientation. It provides an organization with data on the magnitude of some problems that plague the delivery of outpatient care. These problems afflict the processes of referral, results management, and test ordering. The organization may decide to make IT investments in an effort to reduce or eliminate these problems. For example, outpatient computerized provider order entry could reduce the prevalence of adverse drug events. Reminders in an electronic medical record system could help the physician remember to order cholesterol tests for patients at high risk of hypercholesterolemia.

When this vector is used, the IT agenda is driven at least in part by a relentless, year in, year out focus on improving core processes and information management needs.

IT Strategies Based on Examination of the Role of New Information Technologies

The third vector involves considering how new IT capabilities may enable a new IT agenda or significantly alter the current agenda. For example, telemedicine capabilities may enable the organization to consider a strategy that it had not previously considered, such as extending the reach of its specialists across the globe, or may alter its approach to achieving an existing strategy, so that, for example, it relies less on specialists visiting regional health centers and more on teleconsultation. Wireless technologies may enable the organization to consider applications that previously were not effective because there was no good way to address the needs of the mobile worker—for example, medication administration systems can now be used at the bedside rather than requiring the nurse to return to a central work area to document administration.

TABLE 12.2. SUMMARY OF THE SCOPE OF OUTPATIENT CARE PROBLEMS.

For Every:	There Appear to Be . . .
1,000 patients coming in for outpatient care	14 patients with life-threatening or serious ADEs
1,000 outpatients who are taking a prescription drug	90 who seek medical attention because of drug complications per 1,000 prescriptions written
1,000 prescriptions written	40 with medical errors
1,000 women with a marginally abnormal mammogram	360 who will not receive appropriate follow-up care
1,000 referrals	250 referring physicians who have not received follow-up information 4 weeks later
1,000 patients who qualified for secondary prevention of high cholesterol	380 will not have a LDL-C, within 3 years, on record

In this vector the organization examines new applications and new base technologies and tries to answer the question, Does this application or technology enable us to advance our strategies or improve our core processes in new ways? For example, applications that support communication between physician and patient through the Internet might lead the organization to think of new approaches to providing feedback to the chronically ill patient. Holding new technologies up to the spotlight of organizational interest can lead to decisions to invest in a new technology.

An extreme form of this mechanism occurs when a new technology or application suggests that fundamental strategies or even the organization's existence may be called into question or need to undergo significant transformation. Although IT-induced transformation is rare in health care, it is being seen in other industries. The Internet, for example, is transforming and in some case challenging the existence of a range of companies that distribute *content*. Examples are companies such as bookstores, record and CD stores, publishers, travel agents, and stockbrokers.

IT Strategies Based on Assessment of Strategic Trajectories

Organization and IT strategies invariably have a fixed time horizon and fixed scope. These strategies might cover a period of time two to three years into the future. They

outline a bounded set of initiatives to be undertaken in that time period. Assessment of strategic trajectories asks the question, What do we think we will be doing after that time horizon and scope? Do we think that we will be doing very different kinds of things, or will we be carrying out initiatives similar to the ones that we are doing now?

For example, we might be planning to introduce decision support into our CPOE application. This decision support would point out drug-drug interactions and drug-lab test interactions. Answering the question about trajectories for that decision support might indicate to us that patient genetic information will eventually need to be part of our decision-support approach because genetic makeup can have a significant impact on patient tolerance of a drug. Or we might be in the process of implementing electronic data interchange to support the basic payer-provider transactions—for example, eligibility determination and claims submission. We expect that this support will significantly improve the efficiency of these transactions. Answering the question about trajectories for systems that link the provider to the payer might indicate that we are heading into a time of ever-tighter integration between payer and provider information systems. This integration might become so strong that we should examine the merger of our master patient index with the payer subscriber database in order for both provider and payer to eliminate problems associated with misidentification of patients or subscribers.

The trajectory discussion may be grounded on IT applications, as in the examples just given. It may also be grounded on today's organization, with an effort being made to envision the organization as it would like to be in the future. That vision may point to IT strategy directions and needs. For example, a vision of an organization with exceptional patient service might indicate the need to move toward applications that enable patients to book their own appointments.

The strategic trajectory discussion can be highly speculative. It might be so forward looking and speculative that the organization decides not to act today on its discussion. Yet it can also point to initiatives to be undertaken within the next year to better understand this possible future and to prepare the organization's information systems for it. For example, if we believe that our information systems will eventually need to store genetic information, it would be worth understanding whether the new clinical data repository we will be selecting soon will be capable of storing these data.

IT Strategies Based on Fundamental Views About Competition or Organizations

Several IT strategic-planning methodologies are based on fundamental views of the nature of organizations, organization processes, or competition. Often these views are originally presented in literature that examines management and strategy issues in general and then are adapted for use in IT strategic planning.

The competitive forces model (Porter, 1980) is an example of a fundamental view, and we'll use it to illustrate this vector. The competitive forces model examines forces that shape the competitive environment and hence an industry's (and its member organizations') profitability. Porter (1980) identifies five competitive forces that determine an industry's profitability: the bargaining power of buyers, the bargaining power of suppliers, the threat of new entrants, the threat of substitute products, and the rivalry among existing competitors.

Consider some health care examples of these forces. The competitive strength of a managed care organization is weakened if employers (buyers of insurance) have significant bargaining power. If a hospital has already made a significant commitment to an IT vendor, then it has a difficult time negotiating a reduction in fees because the vendor (the supplier) knows that the hospital is unlikely to deinstall a large number of applications. A community hospital's laboratory might be threatened by the advent of free-standing commercial laboratories in its region. A breakthrough in outpatient surgery (a substitute product) could mean that lucrative inpatient surgery volume will diminish. Clearly, a market with several, strong nursing home competitors will lead to smaller margins for all nursing home organizations than will a market with only weak competition.

In order to gain a competitive advantage, companies must devise methods to counter each of these forces. IT can be one of those methods. Conversely, the use of IT by others might threaten an organization's competitive position. For example, the bargaining power of patients (buyers) over providers and payers may be increased by consumer-oriented Web sites that rate provider quality. The barriers that new entrants in some industries must surmount have increased due to the large investments needed to remain on the cutting edge of IT—for example, organizations often join integrated delivery systems because of the capital cost of the information technology viewed as necessary in order to compete. The Internet can reduce the role of traditional channels, such as the referring physician (a buyer of specialty services), by supporting the patient's ability to find and access a specialist. Internet-based health insurance companies, often focusing on supporting a movement to defined contributions, can be viewed as offering a substitute product and thus are a threat to a traditional payer.

IT can also enable the creation of new health care industries and businesses—for example, Internet-based health care consumer content, health insurance products, and providers of second opinions—all of which alter the rivalry force.

Porter's framework could guide the development of IT strategy by encouraging the organization to ask questions such as: How can we apply IT to strengthen our role as a supplier? (for example, by providing access to clinical systems to our referring physicians), or, Can we use IT to develop substitute products? (for example, by using telemedicine as a replacement for face-to-face interaction with a specialist). The process of arriving at an IT strategic plan using the competitive forces framework requires a

very different conversation from the conversation that centers on the organization's published strategic plan.

Vector Summary

Developing IT alignment and strategy requires the convergence of five vectors of thinking and discussion, although the fifth vector (IT strategy based upon fundamental views about competition and organizations) is not commonly used in health care. These vectors bring multiple orientations to strategy formulation and implementation, and each often results in a different management discussion.

Methodologies have been developed to help guide organizations through the necessary discussions. Organizations commonly use consultants for this purpose; they can provide not only methodologies but also perspectives on new IT and the IT agenda and the experiences of other health care organizations.

Whether methodologies or consultants are used or not, the development of the IT strategy is not a cookbook exercise. At its core the alignment with organization strategy is achieved because smart, thoughtful organization leadership takes the time to discuss the IT strategy. On the one hand alignment sounds very simple—smart people talk about it. On the other hand such simplicity means that there is a significant amount of *art* to this process. In general the accountability for developing an aligned IT agenda should rest with the CIO.

IT Asset and Governing Concepts

The discussion of vectors and alignment up to this point has focused generally on the development of an application agenda as the outcome. In other words, the completion of the IT strategy discussion is an inventory of systems such as the EMR system, customer relationship management system, and clinical laboratory system that are needed to further overall organization strategies. However, the application inventory is a component of the larger idea of the IT asset. And in addition to the IT asset, the IT strategy conversation must address governing concepts. These areas are discussed in the following sections.

IT Asset

The *IT asset* is composed of those IT resources that the organization has or can obtain and that are applied to further the goals, plans, and initiatives of the organization. The IT strategy discussion identifies specific changes or enhancements to the composition of the asset—for example, the implementation of a new application—and general

properties of the asset that must exist—for example, high reliability of the infrastructure. The IT asset has five components: applications, infrastructure, data, IT staff, and IT governance.

Applications. Applications are the systems that users interact with—for example, scheduling, billing, and electronic medical record systems. In addition to developing an inventory of applications, the organization may need to develop strategies regarding properties of the overall portfolio of applications.

For example, if the organization is an integrated delivery system, decisions will need to be made about the degree to which applications should be the same across the organization. E-mail systems ought to be the same, but is there a strategic reason to have the same clinical laboratory system across all hospitals? Or should an organization buy or build its applications? Building applications is risky and often requires skills that most health care organizations do not possess. However, internally developed applications can be less expensive and can be tailored to an organization's needs.

Strategic thinking may center on the form and rigor of the justification process for new applications. Formal return on investment analyses may be emphasized so that all application decisions will emphasize cost reduction or revenue gain. Or the organization may decide to have a decision process that takes a more holistic approach to acquisition decisions so that factors such as improving quality of care must also be considered.

In general, strategy discussions surrounding the application asset as a whole focus on a few key areas:

- *Sourcing.* What are the sources for our applications? And what criteria determine the source to be used for an application? In other words, should we buy or build applications? If we buy, should we get all applications from the same vendor or will we use a small number of approved vendors?
- *Application uniformity.* If we are a large organization with many subsidiaries or locations, to what degree should our applications be the same at all locations? If some have to be the same but some can be different, how do we decide where we allow autonomy? This discussion is often involves a trade-off between local autonomy and the central desire for efficiency and consistency.
- *Application acquisition.* What processes and steps should we use when we acquire applications? Should we subject all acquisitions to rigorous analyses? Should we use a request for proposal for all application acquisitions? This discussion is generally an assessment of the extent to which the IT acquisition process should follow the degree of rigor applied to non-IT acquisitions (of diagnostic equipment, for example).

Infrastructure. Infrastructure needs may arise from the strategic-planning process. An organization desiring to extend its IT systems to community physicians will need to ensure that it can deliver low-cost and secure network connections. Organizations placing significant emphasis on clinical information systems must ensure very high reliability of their infrastructure; computerized provider order entry systems cannot go down.

In addition to initiatives designed to add specific components to the infrastructure—for example, new software to monitor network utilization—architecture strategies will focus on the addition or enhancement of broad infrastructure capabilities and characteristics.

Capabilities are defined by completing this sentence: “We want our applications to be able to . . .” We could complete that sentence with phrases such as “be accessed from home,” “have logic that guides clinical decision making,” or “share a pool of consistently defined data.”

Characteristics refer to broad properties of the infrastructure, such as reliability, agility, supportability, integrability, and potency. An organization may be heading into the implementation of mission-critical systems and hence must ensure very high degrees of reliability in its applications and infrastructure. The organization may believe that it is in the middle of a large amount of environmental uncertainty and hence must place a premium on agility. The asset plans in these cases involve discussions and analyses that are intended to answer the questions: What steps do we need to take to significantly improve the reliability of our systems? or, If we need to change course quickly, how do we ensure an agile IT response?

Data. Data and information were discussed in Chapters One and Two and data management in Chapter Eight. Strategies surrounding data may center on the degree of data standardization across the organization, accountability for data quality and stewardship, and determination of database management and analyses technologies.

Data strategy conversations may originate with questions such as: We need to better understand the costs of our care. How do we improve the linkage between our clinical data and our financial data? or, We have to develop a much quicker response to outbreaks of epidemics. How do we link into the city’s emergency rooms and quickly get data on chief complaints?

In general, strategies surrounding data focus on acquiring new types of data, defining the meaning of data, determining the organizational function responsible for maintaining that meaning, and integrating existing sets of data and technologies used to manage, analyze, and report data.

IT Staff. IT staff are the analysts, programmers, and computer operators who, day in and day out, manage and advance information systems in an organization. IT staff

were discussed in Chapter Eleven. Alignment discussions may highlight the need to add IT staff with specific skills, such as Web developers and clinical information system implementation staff. Organizations may decide that they need to explore outsourcing the IT function in an effort to improve IT performance or obtain difficult-to-find skills. The service orientation of the IT group may need to be improved.

In general the IT staff strategies focus on the acquisition of new skills, the organization of the IT staff, the sourcing of the IT staff, and the characteristics of the IT department—is it, for example, innovative, service oriented, and efficient?

IT Governance. IT governance is the organizational mechanisms by which IT priorities are set, IT policies and procedures are developed, and IT management responsibility distributed. IT governance will be discussed in Chapter Thirteen.

Governing Concepts

At times, classes of technology, applications, and IT management techniques (which we will refer to collectively as *technologies* in this section) appear to have the potential to make a significant impact on the health care industry and its organizations and on the way those organizations implement and apply information systems. Examples today include the Internet, service-oriented architectures, knowledge management, and electronic medical record systems.

It may not be clear initially how particular technologies could further organization strategies or what their impact could be on the IT asset. As organizations adopt or explore the adoption of technologies, they develop concepts that guide how they think about these technologies, which in turn has great influence over whether and how they will adopt a technology and how they will evaluate its success. For example, there are several ways to think about the Internet and its technologies:

- As a “universal” presentation layer allowing access to a diverse array of legacy systems by a diverse array of workstations.
- As a means of publishing organizational knowledge.
- As a means of finding services and information offered by others.
- As a means of extending an organization’s services into the home.
- As a replacement for electronic data interchange.
- As a distribution channel—for example, one might order a personal computer directly from the manufacturer rather than buying it from a local distributor.

All these concepts are correct in that all can be effective. However, once an organization chooses a concept or concepts it tends to think about the technology in that

way, often to the exclusion of other ways to think about it. Moreover the organization's concept may be wrong or only half-potent. For example, if an organization views Internet technologies solely as a universal user interface, it will miss an extraordinary set of other opportunities for these technologies.

Governing concepts have a considerable impact on all aspects of our lives, and their ramifications are significant. For example:

- One can view the Bible as literal, allegorical, or something that one doesn't think about at all.
- One can view the role of the federal government to be to protect shores and individual freedoms or to compensate for and overcome injustice and deficiencies in the free market.
- One can view an individual's destiny as being heavily influenced by his or her environment and genes, largely determined by the choices he or she makes in life, or preordained by larger forces in the universe.
- One can view the goal of a college education to be preparing for a job, garnering knowledge of one's society and civilization, or attending a prolonged party.

There is no one formula or cookbook for arriving at governing concepts. The strategic-planning vectors discussed earlier in this chapter represent different governing concepts. This chapter will not attempt to present a methodology for concept development. Concepts emerge from complex and not well understood phenomena involving insight, discussions among members of the organization's leadership, examinations of the strategic efforts of others, the organization's successes and failures (and the reasons it assigns for success and failure), and organizational values and history that form the basis for judging views. The basis for concept formation is a small number of questions. These questions are often easy to state. For example:

- What is it about the electronic medical record that makes it important to us?
- Should we view electronic prescribing (the electronic linkage of a provider's medication ordering with the pharmacy benefits manager's eligibility determination function with the retail pharmacy's fulfillment function) as a competitive advantage, or should we view it as a regional utility? If we view it as the former, we should proceed unilaterally. If we view it as the latter, we should put together a regional collaborative to develop it.
- When we say that we want to integrate our systems, what does integration mean to us? Common data? Common interface? Common application logic?
- Should IT be a tightly controlled resource, or should we encourage multiple instances of IT innovation? What would cause us to choose one approach over the other?

Developing thoughtful and insightful answers to questions such as these is difficult. Nonetheless, forming such concepts is critical.

In addition to creating an application inventory, the IT strategy can lead to asset strategies and plans. Strategies may be developed that alter the asset, as a response to questions such as these:

- What is our approach to ensuring that it will become easier to integrate applications?
- What is our approach to attracting and retaining superb IT talent?
- How do we improve our prioritization of IT initiatives?
- Which data should be consistently defined across the organization, and how do we develop those definitions?

In general, significant changes to the IT asset are defined during the alignment discussion as a result of answering two questions:

- Does our IT strategy suggest that we should make major changes to any portion of our IT asset?
- Are there areas of our IT asset that require significant improvements in performance?

A minority of the elements that make up the IT strategy will require the discussion about governing concepts. The IT strategy may be clear and not helped by high-altitude conceptual discussions. If the organization needs a new patient accounting system, it may not gain any ground by examining the conceptual nature of patient accounting systems. That said, it is not easy to know where conceptual discussions might be helpful. In general these discussions may have merit for those elements of the IT strategy that are deemed to be particularly critical, that possess a high degree of uncertainty because they are new to the industry and hence real experience is limited, or that require a very large investment.

A Normative Approach to Developing Alignment and IT Strategy

You may now be asking yourself, How do I bring all of this together? In other words, is there a suggested approach that an organization can take to develop its IT strategy that takes into account these various vectors? And by the way, what does an IT strategic plan look like?

Across health care organizations the approaches taken to developing, documenting, and managing an IT strategy are quite varied. Some organizations have well-developed, formal approaches that rely on the deliberations of multiple committees and leadership retreats. Other organizations have remarkably informal processes—a

small number of medical staff and administrative leaders meet, in informal conversations, to define the organization's IT strategy. In some cases the strategy is developed during a specific time in the year, often preceding the development of the annual budget. In other organizations IT strategic planning goes on all the time, permeating a wide range of formal and informal discussions.

There is no right way to develop an IT strategy and to ensure alignment. However, the process for developing IT strategy should be similar in approach and nature to the process used for overall strategic planning. If the organization's core approach to strategy development is informal, so should be its approach to IT strategy development.

Recognizing this variability, a *normative* approach to the development of IT strategy can be offered.

Strategy Discussion Linkage

Organization strategy is generally discussed in senior leadership meetings. These meetings may be focused specifically on strategy or strategy may be a regular agenda item. These meetings may be supplemented with retreats centered on strategy development and with task forces and committees that are asked to develop recommendations for specific aspects of the strategy—for example, a committee of clinical leadership might be asked to develop recommendations for improving patient safety.

Regardless of their form, the organization's CIO should be present at such meetings or kept informed of the discussion and its conclusions. If task forces and committees supplement strategy development, an IT manager should be asked to be a member. The CIO (or the IT member of a task force) should be expected to develop an assessment of the IT ramifications of strategic options and to identify areas where IT can enable new approaches to strategy. The CIO will not be the only member of the leadership team who will perform this role. CFOs, for example, will frequently identify the IT ramifications of plans to improve claims processing. However, the CIO should be held accountable for ensuring that the linkage does occur.

As strategy discussions proceed, the CIO must be able to summarize and critique the IT agenda that should be put in place to carry out the various aspects of the strategy. Figure 12.2 displays an IT agenda that might emerge from a strategy designed to improve the patient service experience in outpatient clinics. Figure 12.3 displays a health plan IT agenda that could result from a strategy designed to improve patient access to health information and self-service administrative tasks.

IT Liaisons

All major departments and functions—for example, finance, nursing, and medical staff administration—should have a senior IT staff person who serves as the function's point

FIGURE 12.2. IT INITIATIVES NECESSARY TO SUPPORT A STRATEGIC GOAL FOR A PROVIDER.

Strategic Goal

Improve service to outpatients

Problem

- Patients have to call many locations to schedule a series of appointments and services.
- The quality of the response at these locations is highly variable.
- Locations inconsistently capture necessary registration and insurance information.
- Some locations are overcapacity whereas others are underutilized.

IT Solution

- Common scheduling system for all locations.
 - A call center for “one stop” access to all outpatient services.
 - Development of master schedules for common service groups, for example, preoperative testing.
 - Integration of scheduling system with electronic data interchange connection to payers for eligibility determination, referral authorization, and copay information.
 - Patient support material, for example, maps and instructions, to be mailed to patient.
-

of contact. As these functions examine ways to improve their processes—for example, lower their costs and improve their services—the IT staff person can work with them to identify IT activities necessary to carry out their endeavors. This identification often emerges with recommendations to implement new applications that advance the performance of a function, such as a medication administration record application to improve the nursing workflow. Figure 12.4 provides an example of output from a nursing leadership discussion on improving patient safety through the use of a nursing documentation system.

New Technology Review

The CIO should be asked to discuss, as part of the strategy discussion or in a periodic presentation in senior leadership forums, new technologies and their possible contributions to the goals and plans of the organization. These presentations may lead to suggestions that the organization form a task force to closely examine a technology. For example, a multidisciplinary task force could be formed to examine the role of wireless technology in nursing care, materials management, and service provision to referring

FIGURE 12.3. IT INITIATIVES NECESSARY TO SUPPORT A STRATEGIC GOAL FOR A HEALTH PLAN.

Strategic Goal

- Improve service to subscribers
- Reduce costs

Problem

- Subscribers have difficulty finding high-quality health information.
- The costs of performing routine administrative transactions, for example, change-of-address and responses to benefits questions, is increasing.
- Subscriber perceptions of the quality of service in performing these transactions is low.

IT Solution

- A plan portal that provides:
 - Health content from high-quality sources
 - Access to chronic disease services and discussion groups
 - Subscriber ability to use self-service to perform routine administrative transactions
 - Subscriber access to benefit information
 - Functions that enable subscriber to ask questions
 - Plan ratings of provider quality
 - A plan-sponsored provider portal that enables
 - Subscribers to conduct routine transactions with their provider, for example, request appointment or renew prescription
 - Electronic visits for certain conditions, for example, back pain
 - Subscribers to ask care questions of their provider
-

physicians. Table 12.3 provides an example of a review of the potential contribution of wireless technology; various potential uses of wireless technology are assessed according to their expected ability to increase revenue, reduce costs, improve care quality, and improve patient service.

Synthesis

The CIO should be asked to synthesize, or summarize, the conclusions of these discussions. This synthesis will invariably be needed during the development of the annual budget. And the synthesis will be a necessary component of the documentation and presentation of the organization's strategic plan. Table 12.4 presents an example of such a synthesis.

FIGURE 12.4. SYSTEM SUPPORT OF NURSING DOCUMENTATION.

Problem Statement

- Both the admitting physician(s) and nurse document medication history in their admission note.
- Points of failure have been noted:
 - Incompleteness due to time or recall constraints, lack of knowledge, or lack of clear documentation requirements
 - Incorrectness due to errors in memory, transcription between documents, and illegibility
 - Multiple inconsistent records due to failure to resolve conflicting accounts by different caregivers
- Most of the clinical information required to support appropriate clinician decision making is obtained during the history-taking process.

Technology Interventions and Goals

- A core set of clinical data should be made available to the clinician at the point of decision making:
 - Demographics
 - Principle diagnoses and other medical conditions
 - Drug allergies
 - Current and previous relevant medications
 - Laboratory and radiology reports
 - Required information should be gathered only once:
 - Multidisciplinary system of structured, templated documentation
 - Clinical decision-support rules, associated with specific disciplines, to guide gathering
 - Workflow that supports the mobile caregiver with integrated wireless access to clinical information
 - Needed applications could be implemented in phases:
 - Nursing admission assessment
 - Multidisciplinary admission assessment
 - Planning and progress
 - Nursing discharge plan
 - Multidisciplinary discharge plan
-

TABLE 12.3. POTENTIAL VALUE PROPOSITION FOR WIRELESS TECHNOLOGY.

Function	Value			
	Revenue	Cost Savings	Care Quality	Patient Service
Medical information or textbooks	L	L	M	L
Lab test orders	M	L	L	L
Medication orders	H	M	H	M
Results retrieval	L	M	M	L
Patient charting	M	L	M	L
Charge capture	H	M	L	M
Supply management	L	H	L	L

Note: H = High, M = Medium, L = Low.

TABLE 12.4. SAMPLE SYNTHESIS OF IT STRATEGIC PLANNING.

Strategic Challenge	IT Agenda
Capacity and growth management	Emergency department tracking Inpatient electronic bed board Ambulatory clinic patient tracking
Quality and safety	Inpatient order entry Anticoagulation therapy unit On-line discharge summaries Medication administration record
Performance improvement	Registration system overhaul Anatomic pathology Pharmacy Order communication Transfusion and donor services
Budget management and external reviews	Disaster recovery JCAHO preparation Privacy policy review

The organization should expect that the process of synthesis will require debate and discussion—for example, trade-offs will need to be reviewed, priorities set, and the organization's willingness to implement embryonic technologies determined. This synthesis and prioritization process can occur in the course of leadership meetings, through the work of a committee charged to develop an initial set of recommendations, and during discussions internal to the IT management team.

An example of an approach to prioritizing recommendations is to give each member of the committee "\$100" to be distributed across the recommendations. The amount a member gives to each recommendation reflects his or her sense of its importance. For example, a member could give one recommendation \$90 and another

\$10 or give five recommendations \$20 each. In the former case the committee member believes that only two recommendations are important and the first one is nine times more important than the second. In the latter case the member believes that five recommendations are of equal importance. The distributed dollars are summed across the members, with a ranking of recommendations emerging.

For an example of the scoring of proposed IT initiatives, see Figure 12.5. It lists categories of organizational goals—for example, improve service and invest in people—along with goals within the categories. The leadership of the organization, through a series of meetings and presentations, has scored the contribution of the IT initiative to the strategic goals of the organization. The contribution to each goal may be critical (*must do*), *high*, *moderate*, or *none*. These scores are based on data but nonetheless are fundamentally judgment calls. The scoring and prioritization will result in a set of initiatives deemed to be the most important. The IT staff will then construct preliminary budgets, staff needs, and timelines for these projects.

Figure 12.6 provides an overview of the timeline for these initiatives and the cost of each. Management will discuss various timeline scenarios, considering project interdependence and ensuring that the IT department and the organization are not overwhelmed by too many initiatives to complete all at once. The organization will use the budget estimates to determine how much IT it can afford. Often there is not enough money to pay for all the desired IT initiatives, and some initiatives with high and moderate scores will be deferred or eliminated as projects. The final plan, including timelines and budgets, will become the basis for assessing progress throughout the year.

Overall, a core role of the organization's chief information officer is to work with the rest of the leadership team to develop the process that leads to alignment and strategic linkage.

Once all is said and done, the alignment process should produce these results:

- An inventory of the IT initiatives that will be undertaken. These initiatives may include new applications, major enhancements to the infrastructure, and projects designed to improve the IT asset.
- A diagram or chart that illustrates the linkage between the initiatives and the organization's strategy and goals.
- An overview of the timeline and the major interdependencies between initiatives.
- A high-level analysis of the budget needed to carry out these initiatives.
- An assessment of any material risks to carrying out the IT agenda, and a review of the strategies needed to reduce those risks.

It is important to recognize the amount and level of discussion, compromise, and negotiation that go into the strategic alignment process. Producing these results without going through the preceding thoughtful process will be of little real benefit.

FIGURE 12.5. IT INITIATIVE PRIORITIES.

Color Key			Enhances Patient Care Strengthens Community Outreach Strengthens Physician Integration Strengthens Employee Support Enhances Operational Efficiency Minimizes Investment Level Invests in Current Scalable Technology Supports Growth with Strong ROI Addresses Significant System Deficiency Addresses Compliance Issues (Must Do) Mandatory Technology Building Block									
High	Moderate	Must Do	Service	People	Financial	Growth	Quality and Safety	Infra-structure	Overall Priority			
Clinical applications												
1. Physician order entry	✓		✓		✓		✓	✓		Start now		
2. Patient care documentation	✓				✓		✓	✓		Plan it		
3. Clinical data repository			✓		✓		✓			Start now		
4. Computerized medical record	✓		✓		✓					Delay it		
5. Pacs (phase I)					✓		✓			Start now		
6. Expand physician practice mgmt.			✓		✓	✓				Plan it		
7. Departmental systems										Ongoing		
Data integration												
8. Integration engine						✓	✓	✓		Plan it		
Administrative and financial systems												
9. General financials					✓	✓				Plan it		
10. Materials management				✓	✓	✓				Plan it		
11. Scheduling application		✓		✓	✓		✓			Plan it		
12. Decision-support system				✓	✓		✓			Start now		
Emerging technologies												
13. Wireless LAN & WAN			✓		✓	✓	✓			Plan it		
14. Voice recognition			✓		✓	✓				Start now		
Infrastructure												
15. Server consolidations/upgrades								✓		Plan it		
16. Network upgrades								✓		Ongoing		
17. Security: SSO, HIPAA, policies					✓		✓	✓	✓	Plan it		
Governance												
18. Project/change mgmt. office				✓	✓	✓			✓	Start now		
19. US governance (steering, business liaisons, SLAs)				✓	✓	✓				Ongoing		

FIGURE 12.6. PLAN TIMELINES AND BUDGET.

		FY2002 Capital (in \$'000)	FY2003 Capital Expense (in \$'000)		FY2004 Capital Expense (in \$'000)		FY2005 Capital Expense (in \$'000)		Annual Recurring Operate	FY02	FY2003				FY2004				FY2005			
Priority	Funded	Actual	Low	High	Low	High	Low	High		Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Hospital IT Migration Path																						
Clinical Applications																						
1. Physician order entry	Funded	\$ 200		\$ 1,800					\$ 270	1	4	4	4									
2. Patient care documentation	Plan it		\$ 333	\$ 467	\$ 167	\$ 233			\$ 70													
3. Clinical data repository	Start now			\$ 25					\$ 4				1	3	3							
4. Computerized medical record	Delay it									0.5	0.5	0.5	0.5	0.5								
5. PACS (Phase I)	Start now		\$ 500	\$ 500					\$ 75													
6. Expand physician practice management	Plan it				\$ 50	\$ 150				0.5												
7. Departmental systems	Ongoing		\$ 167	\$ 333	\$ 167	\$ 333	\$ 167	\$ 333	\$ 50		1	1	1	1	1	1	1	1	1	1	1	1
Data integration																						
8. Integration engine	Plan it		\$ 100	\$ 200									1	1								
Administrative and financial systems																						
9. General financials	Plan it				\$ 300	\$ 500																
10. Materials management	Plan it				\$ 200	\$ 333	\$ 100	\$ 167							1	2	2					
11. Scheduling application	Plan it				\$ 75	\$ 150	\$ 225	\$ 450														
12. Decision-support system	Start now	\$ 100	\$ 50						8													
Emerging technologies																						
13. Wireless LAN & WAN	Plan it								\$ 75													
14. Voice recognition	Start now	Pending	\$ 100	\$ 300	\$ 167	\$ 667	\$ 83	\$ 333	\$ 45													
Infrastructure																						
15. Server consolidations or upgrades	Plan it		\$ 250	\$ 500					\$ 75													
16. Network upgrades	Ongoing	Funded	\$ 100	\$ 33	\$ 133	\$ 33	\$ 133	\$ 33	\$ 20													
17. Security- SSO, HIPAA, policies	Plan it		\$ 33	\$ 67	\$ 17	\$ 33			\$ 10		1	1	1	1	1	1	1	1	1	1	1	1
Governance																						
18. Project or change management office	Start now	Funded	\$ 10	\$ 20					\$ 3													
19. US governance (steering, business liaisons, SLAs)	Ongoing	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A		1	3	3	3	3	3	3	3	3	3	3	3

Note: “Annual Recurring” is the ongoing operating cost of the system. Approximate project timelines are shown in the right-hand columns. Numbers below the timeline headings indicate the number of IT staff (0.5 and so forth) needed to implement each project.

Challenges of IT Strategy and Alignment

Creating IT strategy and alignment is a complicated organization process. The following sections present a series of observations about that process.

Persistence of the Alignment Problem

Despite the apparent simplicity of the normative process we have described and the many examinations of the topic by academics and consultants, achieving IT alignment has been a top concern of senior organizational leadership for several decades. The annual Computer Sciences Corporation survey of IT management issues finds that aligning IT with the rest of the organization is consistently a major IT challenge (Computer Sciences Corporation, 2001). There are several reasons for the persistent difficulty of achieving alignment (Bensaou & Earl, 1998):

- Business strategies are often not clear or are volatile.
- IT opportunities are poorly understood.
- The organization is unable to resolve the different priorities of different parts of the organization.

Weill and Broadbent (1998) note that effective IT alignment requires that organizational leadership clearly understand and strategically and tactically well integrate (1) the organization's strategic context (its strategies and market position), (2) the organization's environment, (3) the IT strategy, and (4) the IT portfolio (for example, the current applications, technologies, and staff skills). Understanding and integrating these four continuously evolving and complex areas is exceptionally difficult.

At least two more reasons can be added to this listing of factors that make alignment difficult:

- The organization finds that it has not achieved the gains, apparently achieved by others, that it has heard or read about, nor have the promises of the vendors of the technologies materialized.
- Often the value of IT, particularly infrastructure, is difficult to quantify, and the value proposition is fuzzy and uncertain.

In both these cases the organization is unsure whether the IT investment will lead to the desired strategic gain or value. This is not strictly an alignment problem. However, alignment does assume that the organization believes that it has a reasonable ability to achieve desired IT gains. We will discuss the IT value challenge in Chapter Fifteen.

The Limitations of Alignment

As we shall also see in Chapter Thirteen, although alignment is important it will not guarantee effective application of IT. Planning methodologies and effective use of vectors cannot, by themselves, overcome weaknesses in other factors that can significantly diminish the likelihood that IT investments will lead to improved organization performance. These weaknesses include poor relationships between IT staff and the rest of the organization, inadequate technical infrastructure, and ill-conceived IT governance mechanisms. IT strategy also cannot overcome unclear overall strategies and cannot necessarily compensate for material competitive weaknesses.

If one has mediocre painting skills, a class on painting technique will make one a better painter but will not turn one into Picasso. Similarly, superb alignment techniques will not turn an organization limited in its ability to implement IT effectively into one brilliant at IT use. Perhaps this reason, more than any other, is why the alignment issue persists as a top-ranked IT issue. Organizations are searching for IT excellence in the wrong place; it cannot be delivered purely by alignment prowess.

Alignment at Maturity

Organizations that have a history of IT excellence appear to evolve to a state where their alignment process is “methodology-less.” A study by Earl (1993) of organizations in the United Kingdom with a history of IT excellence found that their IT planning processes had several characteristics:

IT planning was not a separate process. IT planning and the strategic discussion of IT occurred as an integral part of the organization’s strategic-planning processes and management discussions. In these organizations, management did not think of separating out an IT discussion during the course of strategy development any more than it would run separate finance or human resource planning processes. IT planning was an unseverable, intertwined component of the normal management conversation. This would suggest not having a separate IT steering committee. (IT steering committees will be discussed in Chapter Thirteen.)

IT planning had neither a beginning nor an end. In many organizations, IT planning processes start in a particular month every year and are completed within a more or less set period. In the studied organizations, the IT planning and strategy conversation went on all the time. This does not mean that an organization doesn’t have to have a temporally demarked, annual budget process. Rather it means that IT planning is a continuous process reflecting the continuous change in the environment and organizational plans and strategies.

IT planning involved shared decision making and shared learning between IT and the organization. IT leadership informed organizational leadership of the potential contribution

of new technologies and the constraints of current technologies. Organizational leadership ensured that IT leadership understood the business plans and strategies and their constraints. The IT budget and annual tactical plan resulted from shared analyses of IT opportunities and a set of IT priorities.

The IT plan emphasized themes. A provider organization may have themes of improving care quality, reducing costs, and improving patient service. During the course of any given year, IT will have initiatives that are intended to advance the organization along these themes. The mixture of initiatives will change from year to year, but the themes endure over the course of many years. Because themes endure year after year, organizations develop competence around these themes. They become, for example, progressively better at managing costs and improving patient service. This growing prowess extends into IT. Organizations become more skilled at understanding which IT opportunities hold the most promise and at managing the implementation of these applications. And the IT staff become more skilled at knowing how to apply IT to support such themes as improving care quality and at helping leadership assess the value of new technologies and applications.

IT Strategy Is Not Always Necessary

There are many times in IT activities when the goal, or the core approach to achieving the goal, is not particularly strategic, and strategy formulation and implementation are not needed. Replacing an inpatient pharmacy system, enhancing help desk support, and delivering Internet access organization-wide, although requiring well-executed projects, do not always require leadership to engage in conversations about organizational goals or to take a strategic look at organizational capabilities and skills. Such discussions would produce little substantive change in the organization's understanding of what it had to do and how it should go about doing it.

There are many times when there is little likelihood that the way an organization achieves a goal will create a distinct competitive advantage. For example, an organization may decide that it needs to provide personal digital assistant (PDA) support to its staff, but it does not expect that that support, or its implementation, will be so superior to a competitor's PDA support that an advantage accrues to the organization.

Much of what IT does is not strategic nor does it require strategic thinking. Many IT projects do not require hard looks at organization mission, thoughtful discussions of fundamental approaches to achieving organizational goals, or significant changes in the IT asset.

IT Alignment and Strategy Summary

The development of IT alignment and strategic linkage is a complex undertaking. Five vectors, each complex, must converge. Organization strategy is often volatile and

uncertain and will invariably be developed in multiple forums, making it difficult to have a static, comprehensive picture of the strategy. The ability of IT to support a strategy can be unclear and the trade-offs between IT options can be difficult to assess. The complexity of this undertaking is manifest in the frequent citing of IT alignment in surveys of major organizational issues and problems. There are no simple answers to this problem. At the end of the day, good alignment requires talented leadership (including the CIO) that has effective debates and discussions regarding strategies and that has very good instincts and understandings about the organization's strategy and the potential contribution of IT.

It appears that organizations that are mature in their IT use have evolved these IT alignment processes to the point where they are no longer distinguishable as separate processes. This observation should not be construed as advice to cease using planning approaches or disband effective IT steering committees. Such an evolution, to the degree that it is normative, may occur naturally, just as kids will eventually grow up (at least most of them will).

Information Technology as a Competitive Advantage

Competitive strategy involves identifying goals in ways that are materially superior to the ways that a competitor has defined them (formulation). It also involves developing ways to achieve those goals and capabilities that are materially superior to the methods and capabilities of a competitor (implementation) (Lipton, 1996). For example, our chief competitor and we may both decide to create a network of primary care providers. However, we might believe that we can move faster and use less capital than our competition does if we contract with existing providers rather than buy their practices. Or we and our competition may both have a mission to deliver high-quality care, but our competitor has decided to focus on selected carve-outs or *focused factories* (Herzlinger, 1997) while we attempt to create a full-spectrum care delivery capacity.

Competitive strategy should attempt to define superiority that can be sustained. For example, we may believe that if our organization moves quickly, it can capture a large network of primary care providers and limit the ability of the competition to create its own network. Being *first to market* can provide a sustainable advantage, although no advantage is sustainable for long periods of time. Similarly, an organization with access to large amounts of capital can have an advantage over an organization that does not. Wealth can provide a sustainable advantage.

As organizations examine strategies and capabilities, an entirely reasonable question is, Can the application of information technology provide a competitive advantage to an organization? Over the last two decades, across a wide range of industries, answers to this question have been explored and developed, most recently through the

lens of the Internet (see, for example, Porter, 2001). Perhaps, as a result of continued evolution of the technology and continued transformation of industries and economies, answers to such questions will always be explored.

These explorations have examined uses of IT that are now legendary; the American Airlines SABRE system for travel reservations, the American Hospital Supply ASAP system for hospital supply ordering, the Federal Express suite of applications for tracking packages, and the Amazon.com approach to Internet-based retailing. In these cases and others an organization was able to achieve an advantage over its competitors through the thoughtful application of IT. Consider these brief overviews of the competitive use of IT by Harrah's Entertainment, Enterprise Rent-a-Car, and Con-Way Transportation Services.

Perspective: Con-Way Transportation Services

A subsidiary of California-based CNF Inc., Con-Way Transportation Services, Inc., is a \$2 billion transportation and services company that provides time-definite and day-definite freight delivery services and logistics for commercial and industrial businesses. A leader in less-than-truckload (LTL) shipping, Con-Way boasts more next-day delivery combinations than any other LTL carrier, and 99 percent on-time reliability in next-day services.

The key to Con-Way's success was the development and implementation of an automated line-haul system. Born out of what was thought to be a logistically and financially impossible task, the system optimizes personnel, equipment, and individual routes for the nighttime movement and timely relay of freight shipments in the United States and Canada. Built around Con-Way's successful core business model and designed using historical performance, human intuitive skills and experience, and selected iterative processes including linear programming, the system transformed a tedious, expensive, and time-consuming manual process into an efficient, automated process that completely routes over 95 percent of each day's shipments in about seven minutes.

The automated line-haul system has given Con-Way several competitive advantages in the industry, some of which were not even foreseen:

- *Dispatch personnel management.* Originally, dispatcher positions were difficult to fill, and new dispatchers had a long learning curve, sometimes as long as eighteen months. The procedures and business rules the dispatchers followed were undocumented, making the company uncomfortably dependent on the knowledge in the dispatchers' heads. The automated system completes the dispatchers' jobs faster and more consistently, letting dispatchers use their time to troubleshoot problems that could jeopardize on-time delivery. Con-Way has been able to reduce its dispatch personnel by three people (through attrition) and can keep the group small as it adds business.

- *Customer benefits.* Con-Way was able to extend its cutoff time for customers requesting overnight shipments. This allows customers to submit orders right up until the end of the business day, which gives Con-Way a competitive advantage because businesses don't want to arrange their activities around shippers' schedules. Additionally, the new system, in coordination with the work of dispatch personnel in troubleshooting problems such as bad weather and road closures, has attained a 99 percent on-time delivery rate.
- *Efficiency.* The line-haul automation system has seen efficiency improvements of 1 percent to 3 percent over the results achieved with manual route planning. Although a modest improvement by industry standards, the incremental effect has resulted in savings of \$4 million to \$5 million annually from paying fewer drivers, moving trucks fewer miles, packing more freight per trailer, and reducing damage from rehandling freight.

Con-Way plans to expand its automated system into other business units, including Con-Way Western Express and Con-Way Southern Express, and is expecting to generate additional operational savings and customer conveniences.

Adapted from Pastore, 2003

Perspective: Harrah's Entertainment

A leader in the gaming industry, Harrah's Entertainment operates twenty-six casinos in thirteen states under the brand names of Harrah's, Rio, Harvey's, and Showboat. As one of the most recognized names in an overwhelmingly competitive industry, Harrah's is focused on building loyalty and value for its customers, shareholders, employees, business partners, and communities by being the most service-oriented, technology-driven, geographically diversified company in gaming.

In an industry where it is hard for one casino to differentiate itself from another, Harrah's has made the important decision to put its dollars into building customer loyalty rather than high-priced themed casinos. It is Harrah's belief that customer demand is stimulated by a company knowing its customers, not building an attractive spectacle. To do this, Harrah's invested \$30 million into WINet (Winner's Information Network) to advance its customer relationship management (CRM) strategy through its Total Rewards Program.

Before the advent of WINet, each Harrah's casino operated independently of the others, with each having its own rewards program—just like every other casino in the country. Each of the casinos had its own information systems that tracked customer data, but none of them were linked or shared information with each other. Harrah's felt it could gain a competitive advantage in the gaming industry by capitalizing on player loyalty. To that end, WINet was developed to standardize and connect the information systems throughout all its casinos, tracking and sharing information about customers and their gaming preferences and practices.

Through WINet, players who were part of Harrah's Total Rewards Program could use their player's card at any of Harrah's casinos throughout the country. In return, Harrah's was able to capture information about its players to use in direct marketing, promotions, contests, customer service, and predictive modeling. Additionally, Harrah's was able to save over \$20 million per year on its overall costs and increase same-store sales growth. The number of customers playing at more than one Harrah's casino increased by 72 percent, and cross-market revenues increased from \$113 million to \$250 million.

Harrah's strategic use of information technology has made other industry players take notice. Harrah's is taking steps to solidify its competitive advantage by patenting the innovative technology that has given it the edge to become a leader in the cut-throat gaming industry.

Adapted from Levinson, 2001

Perspective: Enterprise Rent-a-Car

A leader in the car and truck rental industry, Enterprise Rent-a-Car has more than 530,000 cars in its fleet in over 5,000 locations in five countries. With over 50,000 employees, Enterprise has annual revenues over \$6 billion. Enterprise is focused on providing excellent customer service, as one of its core values, by listening and acting on customer feedback.

Enterprise has been able to remain the leading rental car company in part through its innovative use of information technology to improve customer service and enhance the efficiency of core processes. Ninety-five percent of Enterprise's business comes through local rentals, of which a significant number are replacement rentals, paid for by insurance companies on behalf of drivers whose cars have been in accidents and need to be repaired. In order to make this process efficient and customer friendly, Enterprise developed an Internet-based system called ARMS (Automated Rental Management System) that allows Enterprise and its customers to streamline and automate a once-tedious, time- and resource-consuming process.

The concept of ARMS is simple, but its effect on the car rental industry has been staggering. The insurance company, the repair shop, and the Enterprise rental center are brought together through the Enterprise-supported ARMS Internet site. The insurance company logs into the Web site to search for and make a reservation for its policyholder, the driver whose car needs to be repaired. The driver simply picks up and uses the rental car while his or her car is at a repair shop. Meanwhile, the repair shop updates the status of that car daily until the repair is complete. The repair shop then sends a message to ARMS, which sends a message to the insurance company, who calls the driver with the information that the car is ready. The driver returns the rental car and is driven to the repair shop to pick up his or her own car. Meanwhile, a bill is generated and sent to the insurance company for payment.

Having invested \$28 million to develop and implement ARMS, which has an annual maintenance cost of \$7.5 million, Enterprise processes more than \$1 billion in

transactions through the system, which is used by twenty-two of the nation's twenty-five biggest insurance companies (and by over 150 insurance companies in all), more than doubling its business with certain companies since the advent of ARMS. Moreover, insurance companies are doing more business with Enterprise because the insurance industry saves between \$36 million and \$107 million annually due to shorter rental times (due to eliminating phone calls to Enterprise and repair shops and to eliminating time-consuming paperwork), and shorter repair times (because mechanics don't have to continuously field phone calls from the insurance company).

Adapted from Berkman, 2002

Improving competitive position is a critical element of all strategy discussions. The question to be answered is, What have these experiences taught us about the role of IT as a competitive weapon?

Core Sources of Advantage

The experiences just described and similar experiences among other organizations have led to a series of observations and conclusions about the use of IT to provide a competitive advantage.

In most cases, organizations seeking a competitive advantage through IT, use it to

- Leverage organization processes
- Enable rapid and accurate provision of critical data
- Enable product and service differentiation and occasionally creation
- Support the alteration of overall organizational form or characteristics

Leveraging Organization Processes. IT can be applied in the effort to improve organization processes by making them faster, less error prone, less expensive, more convenient, and available at more times and places. In effect, the *transaction cost* of the process, from the customer's perspective, has been reduced. Examples abound:

- Third-party payer Web sites make the process of enrollment and benefit determination more convenient.
- Accounts receivable applications make accounting processes less expensive and faster.
- Electronic medical record systems make the process of accessing information about a patient's prior encounters more efficient.

These examples and countless others have highlighted several process lessons.

IT leverage of processes is most effective when the processes being leveraged are critical, core processes that

- Are used by customers to judge the performance of the organization
- Define the core business of the organization

Patients are more likely to judge a provider organization by its ambulatory scheduling processes and billing processes than by its accounts payable and human resource processes. Moreover, certain attributes of these processes and their end products matter more than other attributes. For example, patients may judge appointment availability as more important than the organization's ability to process no-shows.

Making diagnostic and therapeutic decisions is a core provider organization process; a process that is essential to its core business. It is unlikely that there are a large number of organization processes that have no bearing on and make no contribution to organizational performance. However, there are processes that are more essential than others to the mission of the organization and its goals. Customers may have limited ability to judge or evaluate these processes. For example, most patients cannot judge how well a provider organization makes diagnostic and therapeutic decisions, despite the growing use and sophistication of quality measures.

Keen (1997) defines the importance of processes along two dimensions. *Worth* is a measure of the difference between the cost of a process and the revenue it generates. *Salience* is a measure of the degree to which a process is critical to the identity of an organization or is critical to its effectiveness. The referral process may have high worth. The ambulatory scheduling process may be a critical contributor to the organization's efforts to be identified as "patient friendly." Medical management may be critical to a payer's effectiveness.

IT can enable an organization to materially alter the nature of its processes. For example, technology can enable processes or business activities to be extended over a wider geography than the immediate service area. Telemedicine enables consultation to occur with patients across the globe. The Internet enables patients in many countries to enroll in clinical trials. IT can give subscribers a self-service option for resolving claims and benefits issues.

Processes can be altered or created in a manner that enables the organization to craft or significantly enhance strategic partnerships with other organizations. A process can be moved from one organization to another, as it is in outsourcing. For example, a hospital and a managed care organization, rather than conducting credentialing separately, could share that responsibility. Providers and materials suppliers have established just-in-time inventory replenishment processes that move the inventory function from the provider to the supplier. These approaches and others are predicated on a strong IT core.

Process reexamination should accompany any effort to apply IT to process improvement. If underlying problems with processes are not remedied, the IT investment can be wasted or diluted. IT applications may result in existing processes

continuing to perform poorly only faster. Moreover, it can be harder to fix flawed processes after the application of IT because the IT-supported process now has an additional source of complexity, cost, and ossification to address, the “new computer system.” Process reexamination, addressed elsewhere in this book, can range from incremental, although valuable, change to more radical reengineering.

In addition to the examination and improvement of the mechanics of the process that is the target of the information system, the reexamination should question whether the process is defined correctly. Process definitions often incorporate the mechanics of the process into the core definition of the process, inappropriately narrowing the reexamination effort. For example:

- A definition of a process as “obtaining cash from the bank” might lead a reengineering effort to place ATMs only at the bank. Such ATMs might ease the burden of standing in line on a Saturday morning and hence be viewed as an improvement. However, a statement of the process as “obtaining cash” might lead one to consider all the places where people need cash—malls, theaters, and airports. This might result in the placement of ATMs in many and varied locations, leading to a far more powerful improvement in the process. Similarly, a statement of this process as “buying something” might lead one to create debit cards as cash surrogates.
- A definition of a process as “obtaining a referral number” might lead one to construct an EDI link between the managed care application and the systems in the physician’s office. A statement of this process as “managing referrals” might lead one to abandon entirely the process of obtaining the referral number.

Rapid and Accurate Provision of Critical Data. Organizations define critical elements of their plans, operations, and environment. These elements must be monitored to ensure that the plan is working, service quality is high, the organization’s fiscal situation is sound, and the environment is behaving as anticipated. Clearly, data are required to perform such monitoring.

IT can improve a competitive position by providing such data. Examples abound:

- Gathering data during registration about the patient’s referring physician can help a hospital understand whether its outreach activities and market share growth strategies are working.
- Obtaining data about why subscribers do not reenroll in a health insurance plan aids the plan in identifying major service deficiencies.
- Bar-code scanners at supermarkets and department stores tell product suppliers which products are being purchased. This knowledge can ensure that valuable shelf space is filled with the optimal mix of product. This knowledge can also improve inventory management and manufacturing capacity utilization. Bar-code data in

combination with other data about the customer, obtained when the customer presents a store card to obtain discounts, enables the store and the product manufacturer to understand the demographics of their customers, leading to more focused advertising.

- Provider order entry systems that request the reason or clinical indication for a procedure being ordered not only assist receiving department staff to understand what they are supposed to do but also assist quality assurance and utilization review efforts to understand the dynamics of procedure utilization.

These and other instances of data use have generated several lessons.

Rapid and accurate are relative terms. Data about product movement should be gathered and analyzed in as close to real time as possible because one can change things such as shelf space use almost instantly. Analysis of physician referral patterns need not be done in real time because the organization is unlikely to be able to effect a change in patterns instantly. Complete accuracy about the cost of performing laboratory tests may not be necessary because it can be clear from allocations whether a cost structure is too high or reasonable. High accuracy in linking providers and the medications they order may be critical in order to get provider acceptance of any utilization analyses.

The rapid and accurate gathering of data may be the most significant and important source of a competitive advantage. Having good data about utilization may be more important than efficient ordering processes. Having good data about referring physicians may be more important than an error-free registration process. Knowing the demographics of the customers who consume your snack food, what else they buy when they buy your product, and where and when they buy may be far more important than well-run inventory management. Knowing who your passengers are, their fare tolerance, what time of year they fly, and their destinations may be more important than managing full utilization of the aircraft.

The role of data should not imply that well-run processes are irrelevant. People prefer to obtain services from organizations with well-run processes. Often a well-run, efficient, and convenient process may be necessary to get high-quality data. But in some cases the process is subordinate to the need for the data. There are many examples of the competitive use of IT where the organization, accepting that its rivals will mimic process gains, focuses on the uses of the data. For example, systems to support the making of an airline reservation evolved into the use of the reservation data to develop frequent flyer programs, establish mileage programs linked to credit cards, and engage in fare wars. Those organizations that developed the reservation systems “sold them” to their competitors, recognizing that such a system did not provide a sustainable process advantage.

Product and Service Differentiation. IT can be used to differentiate and customize products and services. Again, examples abound:

- Financial planners may offer prospective customers Web sites that help the customer assess the savings needed to achieve financial goals such as funding college for children or having a certain income at retirement. Customers discover, after running the software, that they will be insolvent within a week after retirement. Fortunately, the financial planner is there to work with the customer to ensure that such a gloomy outcome does not occur.
- Health care providers establish Web sites with information about health news, classes to reduce health risk, new research, and basic triage algorithms. Such information is an effort to differentiate their care from that of others.
- Supermarkets send information to customers about upcoming sales. This information is often based on knowledge of prior customer purchases. Hence a family that has purchased diapers and baby food will be seen as a household with young children. Information about sales on infant products and products directed to young parents will be sent to that household and not to households where a steady pattern of purchasing hot dogs, snack food, and beer indicates a single male. The supermarket is attempting to differentiate its service by helping the household plan its purchases around store specials.

Customization and differentiation often rely on data. Effective customization presumes that we know something about the customer. Differentiation assumes that we know something about the customer's criteria for evaluating our organization so that we can differentiate our processes, products, and services in a way deemed to have value.

Customization and differentiation often center on organization processes. Existing processes can be made unique. New processes can be created. For example, financial services firms enable clients to move their money between money market, stock, and bond accounts by creating new processes that enable such asset movements.

IT has enabled new products and services to be developed and new companies and industries to be formed. For several years around the turn of the millennium, new Internet-based services and companies seemed to be spawned (and to die) daily. Companies that provide comparative analyses of claims and utilization data owe their existence to IT. Capitation as a scheme for financing and managing risk would be extraordinarily difficult without information technology. Several academic medical centers now provide international telemedicine consultations, although it is arguable whether that is an extension of existing service or a new business.

Change in Organizational Form or Characteristics. IT can be used to improve or change certain organizational attributes or characteristics. Such attributes or characteristics might involve service quality orientation, communication, decision making, and collaboration. Consider these examples of using IT to encourage change:

- Most business and medical schools require students to own a personal computer and perform their assignments using the PC and the school's network. This emphasis is intended to accomplish several objectives, one of which is to enhance the student's comfort and skill with the technology.
- Organizations have implemented groupware, such as IBM's Lotus Notes, in an effort to foster collaboration.
- Senior management teams have implemented quality measurement systems in an effort to encourage other managers to be more data driven and focused on key quality parameters, in other words, "to think quality."

The value of such efforts or their impact is often unclear because the organization is changing deep but intangible attributes. For example, becoming more data driven can be a profound change, but it is difficult to measure the value of being data driven or to know if an organization is 50 percent or 80 percent on the way to achieving the desired change. These characteristics tend to be difficult to measure at anything other than a very crude level.

Often a change in organizational characteristics is inadvertent or an unintended consequence of an IT implementation. Electronic mail has been implemented to improve communication, but it has also had the effect of speeding up decision making and altering power structures; staff will, for example, use e-mail to seek information from other staff whom they would feel uncomfortable approaching face to face, using e-mail to schedule a meeting with the chief of medicine, for example.

Sustainability of an Advantage

It is difficult to sustain an IT-enabled or IT-centric advantage. Competitors, noting the advantage, are quick to attempt to copy the application, lure away the original developers, or obtain a version of the application from a vendor who has seen a market opportunity in the success of the original developers. And a sufficient number of these competitors will be successful. Often their success may be less expensive and faster to achieve than the first organization's success was because they learn from the mistakes of the leader. A provider organization that offers Web access to patient results to its referring physicians finds that its competitors will also provide such capabilities. A managed care organization that provides consumer health information and benefits management capabilities to its subscribers finds that its competitors are quite capable of doing the same.

The result can be a form of an IT arms race, a race that provides no advantage for long, a race that you have to run often because customers come to think of the new system as a basic service. No one today would bank at a financial institution that did not offer ATM service.

Knowing that today's IT advantage is tomorrow's core capability possessed by all industry participants, the organization has several strategies that it can adopt:

Attempt to out hustle the competition by aggressive and focused introduction of a series of enhancements to a core system that enables that system to evolve faster than the competition can and to hold a lead.

Freeze the system by ceasing major investments in it and relegating it to the role of a core production system where efficiency and reliability of operation, rather than the possession of superior capabilities, become the objectives. In this case the organization may turn its sights to new systems that attempt to create an advantage in other ways.

Change the basis of competition by using the technology to make the competitive strengths of rivals no longer competitive. Amazon.com attempts to decrease the value of an asset possessed by other retail booksellers, a nationwide network of stores. This network could have been a barrier to entry for Amazon.com; it is expensive to build hundreds of stores. Instead, Amazon.com attempts to make such a network irrelevant and possibly a liability because the network is expensive to maintain.

There are ways that an advantage can be sustained over a prolonged period of time. A single application cannot by itself result in a prolonged sustained advantage. However, an advantage can be sustained for longer than a brief period of time by

- Leveraging some other significant organizational strengths
- Leveraging a well-developed, strong IT asset

Leveraging Other Strengths. Organizations can have strengths that are quite difficult for their competitors to duplicate (Cecil & Goldstein, 1990). Such strengths may include market share, access to capital, brand-name recognition, and proprietary know-how. IT can be used to reinforce or extend such strengths, as in the following examples.

A large integrated delivery system (IDS) and a large retail pharmacy chain, both with significant market shares in a region, may decide to link the IDS's ambulatory care medication order entry system to the pharmacy's dispensing and medication management systems. The IDS's system learns from the pharmacy's system whether the entered medication order was filled, which improves the IDS's medical management programs. The IDS is also able to provide a service to its patients because it can now route a prescription to a pharmacy near a patient's home. The pharmacy is able to channel customers to its stores where it believes that as they pick up medications, they will also make other purchases.

The IDS and the retail pharmacy chain find each other attractive because of their respective shares of the market. The IDS is able to ensure significant geographical coverage for patients who need to fill prescriptions. The pharmacy chain is able to ensure a large volume of customers visiting its stores. Neither party might find another party with less market share as attractive as a partner. For both organizations, this partnership leverages an existing strength of market share.

A well-known academic medical center may be able to leverage its brand name and base of foreign-born physicians, who trained at the medical center, to establish a telemedicine-based international consultation service. It may also be able to leverage its brand name to improve the attractiveness of its consumer-oriented health information Web site. Consumers, confused and worried about the quality of information on the Internet, may take comfort in knowing that information is being generated by a respected source.

These advantages do not result purely from an application system or inherently from process improvement, data gathering, or service differentiation or customization. They result from capitalizing upon some core, difficult-to-replicate strength of the organization, through the application of IT.

Although an organization may have difficult-to-replicate strengths, it should be mindful that IT might also be used to undermine those strengths (Christensen, 2001). For example, most integrated delivery systems have a strength of economies of scope, in other words, they offer a full range of medical services and amortize fixed costs, such as clinical laboratory costs, over this range. When economies of scope exist, the incremental cost of the next medical service is small. Conversely, the incremental savings that result from eliminating a service are small.

If this country moves toward defined contributions as a means of offering health insurance, the employee or patient may be able to select his or her own network of providers, using a Web-based application and bypassing the network defined by the IDS. The employee might select cardiology services from one provider and oncology services from another provider. This *cherry picking* enabled by information technology reduces the advantages of economies of scope. The IDS's revenue from its services that are not picked becomes small, but costs have not been reduced proportionally. The IDS will face competition from organizations that focus on one service line, such as oncology. Compared to the IDS, these focused service providers may also be able to obtain fixed-cost services at less cost. For example, they may obtain testing as a service, supported by IT, from a laboratory service provider.

Leveraging the IT Asset. For most of the health care industry, the technology and applications being implemented today are available to all industry participants, including competitors. Any provider organization can acquire and implement systems from Eclipsys, Cerner, IDX, HBOC, or Siemens. Similarly, why would one payer believe that its claims adjudication system can provide an advantage if its competitor can buy the same system (particularly if the organization has no other advantage—for example, market share—that it is able to leverage with that system)?

An advantage can be obtained if one or both of two things happen. First, one organization might do a more thoughtful and effective job than its competitors do of understanding and then effecting the changes in processes or data gathering associated with the system to be implemented. The application does not provide an advantage,

but the way that it is implemented does. We all see the difference that execution makes every day in all facets of our lives. It is the difference between a great restaurant and a mediocre one or a terrific movie and a terrible one. In neither case is the idea—for example, “let’s make meals and sell them”—or the fact that one executes on the idea—“we’ve hired a cook and purchased silverware”—the advantage. It is the manner of execution that distinguishes.

Second, one organization might be consistently able to outrun the other. If an organization is able to develop means to implement programs and processes faster or cheaper, it may be able to outrun its competition, even if its implementations, one for one, are of no higher quality than its competitors’. Perhaps over a certain period of time one organization implements four applications whereas the other implements three. Or perhaps for a given amount of capital one organization implements five applications whereas the other implements three.

In general, organizations may be able to sustain an IT-based or IT-supported competitive advantage because they have an established and exceptionally strong IT asset—for example, talented IT staff, strong relationships between that staff and the organization, and an agile technical platform (Ross, Beath, & Goodhue, 1996). This asset may be able to consistently and efficiently deliver high-quality applications that enable the organization to improve its competitive position.

The Technology Is a Tool

Information technology can provide a competitive advantage. However, IT has no magic properties. In particular, technology cannot overcome poor strategies, inadequate management, inept execution, or major organizational limitations. For example a system that enables a reduction in nursing staff may not make the salary savings desired if the average nurse’s salary is very high or the staff are unionized. Information systems are tools. If the objectives of a building are not well understood, its design flawed, the carpenter unskilled, and certain tools missing, the quality of the hammer and saw used to build it are irrelevant. In those cases where a significant organizational advantage has been realized, superior strategy, a deep understanding of the business, an ability to execute complex transformations of the business and its core processes, and an ability to capitalize upon IT prowess led to the gains. IT was necessary but not sufficient.

Perspective: How Great Companies Use IT

In his seminal book *Good to Great*, Jim Collins identified companies that made and sustained a transition from being a good company to being a great company. His research noted that these companies had several consistent orientations to IT. They

- Avoided IT fads, but were pioneers in the application of carefully selected technologies.
- Became pioneers when the technology showed great promise in leveraging that which they were already good at doing (their core competency) and that which they were passionate about doing well.
- Used IT to accelerate their momentum toward a being great company, but did not use IT to create that momentum. In other words, IT came after the vision had been set and the organization had begun to move toward that vision. IT was not used to create the vision and start the movement.
- Responded to technology change with great thoughtfulness and creativity, driven by a burning desire to turn unrealized potential into results. Mediocre companies often reacted to technology out of fear, adopting it because they were worried about being left behind.
- Achieved dramatically better results with IT than did rival companies using the exact same technology.
- Rarely mentioned IT as being critical to their success.
- “Crawled, walked and then ran” with new IT even when they were undergoing radical change.

Collins, 2001

In a large number of cases in which IT is used as a competitive weapon, the IT system leverages an existing capability (Freedman, 1991). If that capability is weak, IT may not be able to overcome the weakness. Organizations won't use, for example, a supply ordering system if the supplies are inferior in quality, comparatively expensive, and of limited scope. The experiences of Internet-based e-tailers have highlighted the problems created by sloppy inventory management, poor understanding of customer buying behaviors such as returning purchases, and insufficient knowledge of customer price tolerance.

Referring physicians will not find valuable, and probably will not use, a system that gives them access to hospital data if the consulting physicians at the hospital are remiss in getting their consult notes completed on time or at all. High-quality, comprehensive data on care quality are diminished in value if the organization has limited ability or skill to improve the practice of care.

Other risks that can limit the utility of the IT tool have been seen (Cash, McFarlan, & McKenney, 1992):

- Introducing applications too early, with the result that they have been unable to overcome not-ready-for-prime-time technology and an unreceptive customer environment. Some early EMR implementations suffered this fate.
- Having an inadequate understanding of buying dynamics across market segments. An academic medical center that hopes its consumer-oriented Web page will lead

to increased admissions may not have fully comprehended its own referral process and that 80 percent of referrals to it are made by the patient's physician.

- Being too far ahead of the customer's comfort level. For example, a very large percentage of the public today is uncomfortable with the idea of transmitting individually identifiable health data over the Internet. This discomfort has not been assuaged by the incorporation of advanced security and encryption technologies into these systems.

Finally, the pace of technology evolution is rapid, and new technologies are arriving that enable new ways of supporting processes, gathering data, and differentiating and customizing products and services. In the cases where a significant advantage could be obtained, organizations have been quick to assess new technologies and thoughtful in their application. The incorporation of personal computers and the Web into health care organization activities are examples of technologies that were effectively leveraged when they were new. This behavior suggests that

- Organizations should have a function that scans for new industry-relevant technologies and engages in their evaluation and experimentation.
- To assess new technology well, organizations must develop an understanding of the characteristics of that technology that provide value—for example, what is it about the Web that might produce a significant improvement in care delivery capabilities? This assessment also involves the development of governing concepts.
- Organizations should be careful not to fall in love with their current technology; they need to be able to ruthlessly jettison technology as its ability to provide a competitive distinction wanes.

Singles and Grand Slams

When one looks back at organizations that have been effective at the strategic application of IT over a reasonably long time, one sees what looks like a series of singles punctuated by an occasional leap, a grand slam (McKenney, Copeland, & Mason, 1995). One doesn't see a progression of grand slams or, in the parlance of the industry, *killer* applications (Downes & Mui, 1998). In the course of improving processes, differentiating services, and gathering data, organizations carry out a series of initiatives that improve their performance. The vast majority of these initiatives do not by themselves fundamentally alter the competitive position of the organization, but in the aggregate they make a significant contribution, just as the difference between a great hotel and a mediocre hotel is not the presence of clean sheets or hot water but one thousand little things.

At various points in time the organization has an insight that leads to a major leap in its application of IT to its performance. For example, airlines, having developed

their initial travel reservation systems, continued to improve them. At some point they realized that the data gathered by a reservation system had enormous potency and frequent flyer programs resulted. American Hospital Supply, having developed its supply ordering system, continued to improve it. At some point it realized that it was in a materials management partnership with its hospital customers and not strictly in the supply ordering business. No organization has ever delivered a series of killer, or grand slam, applications in rapid succession.

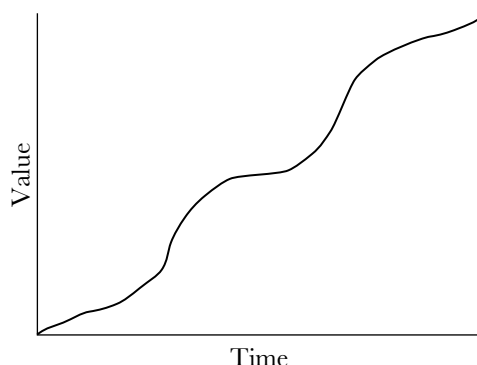
Organizations must develop their IT asset in such a way that they can affect the types of continuous improvements that managers and medical staff will see as possible, day in and day out. For example, in an ideal world an organization would be able to capitalize on the improvements in ambulatory scheduling that a middle manager thinks up and also be able to capitalize on a thousand other good ideas and opportunities. The organization must also develop antennae that sense the possibility of a leap, and the ability to focus that enables it to effect the systems needed to make the leap. Ensuring that these antennae are working is one of the key functions of the chief information officer. The resulting pattern may look like the graph line in Figure 12.7, continuous improvement in performance using IT (singles), punctuated by periodic leaps, or grand slams.

It is also clear that organizations have a limited ability to see more than one leap at a time. Hence they should be cautious about visions that are too visionary or that have a very long time horizon. Organizations have great difficulty understanding a world that is significantly different from the one they inhabit now or that can be only vaguely understood in the context of the next leap. We might understand frequent flyer programs now. But they were not well understood, nor was their competitive value well understood at the time they were conceived. Moreover, the organizational changes required to support and capitalize upon a leap can take years, five to seven years at times (McKenney, Copeland, & Mason, 1995).

Competitive Baggage

The pursuit of IT as a source of competitive advantage can create baggage, or a hang-over. This baggage can occur in several forms.

Significant investment in capital projects, creating an increase in depreciation and an increase in IT operating budgets (depreciation and interest), can erode margins. If several competitors are making similar investments, they may all arrive at a position where the customer sees better service or lower prices, but none of the competitors has developed a system that truly differentiates itself, and they all have reduced their margins in the process. ATMs are an example (Lake, 1998). Customers are better off with ATMs, but no bank distinguishes itself by its ATM capabilities. Banks must now carry the cost of operating the ATM system and funding periodic upgrades in ATM technology. The average ATM machine has a net cost of \$20,000 to \$25,000

FIGURE 12.7. SINGLES AND GRAND SLAMS.

after subtracting fees charged to banks and customers for its use. For the health care provider, investment in Web-based consumer content may have a similar outcome.

Organizations may find themselves in an IT arms race from which prudence has fled, the conversation being replaced by the innate desire to *outfeature* the competitor. The original thoughtfulness surrounding the use of IT to improve processes of care, expand market share, or reduce costs has been replaced by ego.

Governing concepts that were poorly constructed or that fail to evolve can blind organizations to new opportunities. For example, the belief that personal computers were only for hobbyists and had no major role in a large organization was true in 1978 but had become dead wrong by 1984. The belief that the Internet was a realm of interest solely to hackers, voyeurs, and academics also became wrong very quickly. Organizations often hold to beliefs and concepts long after they should be buried. This is particularly problematic when the initial belief led to an IT innovation that was very successful. People and organizations are loath to jettison beliefs that “got them here.” Such blindness has put companies out of business (Christensen, 1997).

IT rigidity can result from poor architecture design or poor partnership selection. Many hospitals have seen, belatedly, the consequences of failure to design for application integration as they attempt to integrate systems acquired over years of a best-of-breed strategy. The pursuit of the advantage to each department of implementing the best product on the market failed to consider the infrastructure properties (the ability to integrate applications efficiently) that would be needed to continue to innovate efficiently later.

Organizations that are overly sensitive to the IT market and grasping for an advantage may pursue new technologies and ideas well before the utility of the idea, if

any, is known. They do not want to be the only organization not pursuing the latest technology or idea and as a result of this nonpursuit destined for the dustbin of also-rans. However, a very large number of ideas, technologies, and management techniques fail to live up to their initial hype. This does not mean they have no utility, just that their utility has not lived up to their press releases. The desire to achieve a competitive advantage can cause organizations to lose their senses, perspective, and at times, appropriate caution.

Finally, extensive use of IT results in dependency on IT. This dependence can affect many resources, from staff to infrastructure. Investment in technologies leaves organizations dependent on their ability to continue to attract and retain scarce and expensive talent. Failure to plan for this dependency can leave the organization exposed when staff turnover occurs. Similarly, organizations that have become reliant on a computerized medical record, with a corresponding intolerance of downtime, are dependent on having a highly reliable and high-performing technical infrastructure. Pursuit of a competitive advantage needs to plan for the dependencies that will be incurred.

Summary

IT planning has several objectives: the alignment of IT with the strategies, plans, and initiatives of the organization; the development of support for the plan; and the preparation of tactical plans.

IT strategies are developed through five vectors. Each vector is complex, and the integration of the vectors is challenging.

IT planning is a very important organization process. However, alignment of IT with the organization has been and remains a major challenge. This process is quite difficult. IT planning prowess cannot guarantee organizational excellence in applying IT.

IT can be very effective in supporting an organization's effort to improve its competitive position. This support generally occurs when IT is employed to leverage core organization processes, support the collection of critical data, customize or differentiate products and services, and transform core characteristics and capabilities.

IT is incapable of providing these advantages by itself. Utility occurs when IT is applied by intelligent and experienced leadership in the pursuit of well-conceived strategies and plans. IT cannot overcome weak leadership, inadequate strategies and plans, or inferior products and services.

Organizations pursuing an IT-supported advantage should be careful of acquiring the baggage that can result: reduced margins with no improvement in competitive position, process ossification, and nonrational pursuit of mirage technologies.

Chapter Twelve: Learning Activities

1. Describe how the EMR can advance the strategies of a health care provider organization.
2. Describe how a customer relationship management system can advance the strategies of a payer organization.
3. Pick an example of a new technology, such as wireless devices. Discuss how this technology might leverage the strategy of a provider or a payer organization.
4. If a health care organization has a strategy of lowering its costs of care, what types of IT applications might it consider? If the organization has a strategy of improving the quality of its care, what types of IT applications might it consider? Compare the two lists of applications.



CHAPTER THIRTEEN

IT GOVERNANCE AND MANAGEMENT

In this chapter we discuss an eclectic but important set of information technology (IT) governance and management processes, structures, and issues. Developing, managing, and evolving IT governance and management mechanisms is often a central topic for organizational leadership. In this chapter we will cover the following areas:

- *IT governance.* IT governance is composed of the processes, reporting relationships, roles, and committees that an organization develops to make decisions about IT resources and activities and to manage the execution of those decisions. These decisions involve such issues as setting priorities, determining budgets, defining project management approaches, and addressing IT problems.
- *IT effectiveness.* Over the years several organizations have demonstrated exceptional effectiveness in applying IT. These organizations include American Express, Bank of America, Schwab, and American Airlines. This chapter discusses what the management of these organizations did that led to such effectiveness. It also examines the attributes of IT-savvy senior leadership.

Lists quoted from Applegate, Austin, & McFarlan, 2003, McGraw-Hill © 2002, are reproduced with permission of The McGraw-Hill Companies.

- *IT budget.* Developing the IT budget is a complex exercise. Organizations always have more IT proposals than can be funded. Some proposals are strategically important and others involve routine maintenance of existing infrastructure, making proposal comparison difficult. Although complex and difficult, the effective development of the IT budget is a critical management responsibility.

IT Governance

IT governance refers to the principles, processes, and organization structure that govern the IT resources (Drazen & Straisor, 1995). When solid governance exists, the organization is able to give a coherent answer to the following questions:

- Who sets priorities for IT, and how are those priorities set?
- What organization structures are needed to support the linkage between IT and the rest of the organization?
- Who is responsible for implementing information systems plans, and what principles will guide the implementation process?
- How are IT responsibilities distributed between IT and the rest of the organization and between centralized and decentralized (local) IT groups in an integrated delivery system?
- How are IT budgets developed?

At its core, governance involves

- Determining the distribution of the responsibility for making decisions, the scope of the decisions that can be made by different organization functions, and the processes to be used for making decisions
- Defining the roles that various organization members and committees fulfill for IT—for example, which committee should monitor progress in clinical information systems, and what is the role of a department head during the implementation of a new system for his or her department?
- Developing IT-centric organization processes for making decisions in such key areas as
 - IT strategy development
 - IT prioritization and budgeting
 - IT project management
 - IT architecture and infrastructure management
- Defining policies and procedures that govern the use of IT. For example, if a user wants to buy a new network for use in his or her department, what policies and procedures govern that decision?

Perspective: The Foundation of IT Governance

Peter Weill and Jeanne Ross have identified five major areas that form the foundation of IT governance. The organization's governance mechanisms need to create structures and processes for these areas.

- *IT principles*: high-level statements about how IT is used in the business.
- *IT architecture*: an integrated set of technical choices to guide the organization in satisfying business needs. The architecture is a set of policies, procedures, and rules for the use of IT and for evolving IT in a direction that improves IT support for the organization.
- *IT infrastructure strategies*: strategies for the existing technical infrastructure (and IT support staff) that ensure the delivery of reliable, secure, and efficient services.
- *Business application needs*: processes for identifying the needed applications.
- *IT investment and prioritization*: mechanisms for making decisions about project approvals and budgets.

Weill and Ross, 2004

Developing and maintaining an effective and efficient IT governance structure is a complex exercise. Moreover, governance is never static. Continuous refinements may be needed as the organization discovers imperfections in roles, responsibilities, and processes.

Governance Characteristics

Well-developed governance mechanisms have several characteristics:

They are perceived as objective and fair. No organizational decision-making mechanisms are free from politics, and some decisions will be made as part of “side deals.” It is exceptionally rare for all managers of an organization to agree with any particular decision. No matter how good an individual is at performing his or her IT governance role, there will be members of the organization who will view that individual as a lower life form. Nonetheless, organizational participants should generally view governance as fair, objective, well reasoned, and having integrity. The ability of governance to govern is highly dependent on the willingness of organizational participants to be governed.

They are efficient and timely. Governance mechanisms should arrive at decisions quickly, and governance process should be efficient, removing as much bureaucracy as possible.

They make authority clear. Committees and individuals who have decision authority should have a clear understanding of the scope of their authority. Individuals who have IT roles should understand those roles. The organization's management must

have a consistent understanding of its approach to IT governance. There will always be occasions where decision rights are murky, roles are confusing, or processes are unnecessarily complex, but these occasions should be few.

They can change as the organization, its environment, and its understanding of technology changes. For example, several organizations spun off portions of their IT groups to create e-commerce departments intended to support the organization's undertakings during the Internet frenzy from 1999 to 2001. This spinning off was an effort to, among other objectives, free e-commerce initiatives from the normal bureaucracy of these organizations' governance structures. This separation was meant to allow the e-commerce groups to operate in "Internet time." These groups have been largely dismantled as a more mature understanding of the role of the Internet developed. Likewise, the growing tendency to intertwine the information systems of partnering organizations—for example, integrating a hospital's materials management systems and the systems of vendors of medical supplies—will require new governance mechanisms that bring representatives from the partnering organizations together to deal with interorganizational IT issues. Governance mechanisms evolve as the technology and the organization's use of IT evolves.

Linkage of Governance to Organization Strategies

Governance structures and responsibility distribution should be heavily influenced by basic strategic objectives. For example, the desire of several provider organizations to be integrated has ramifications for governance design. In this section we will present two examples of governance that is linked to a strategic objective.

Governance to support the *integration* of an integrated delivery system (IDS) might have these characteristics:

- A central IDS IT committee develops the IT priorities, to help ensure the perspective of overall integration, and initiatives that support integration of the system of care are given a higher priority than those that do not.
- A centralized IT group exists, and it has authority over local IT groups.
- IT budgets developed locally are subject to central approval.
- The IT plan specifies the means by which an integrated infrastructure and application suites will be achieved and the boundaries of that plan—for example, local organizations are free to select from a set of patient care system options but, whatever the selection, the patient care system must interface with the IDS clinical data repository.
- Members of the IDS are constrained in their selection of applications to support ancillary departments, having to choose from those on an "approved" list.

- Certain pieces of data—for example, payer class or patient problems—and certain identifiers—for example, patient identifier and provider identifier—have to use a common dictionary or standard.
- All IDS members must use a common electronic mail system.

This approach is designed to ensure that the applications used by all of the organizations within the IDS can be well integrated. This high degree of application integration originates from the IDS strategy of integrating its care. The approach (referring back to our discussion in Chapter Twelve) represents one of the organization's *governing concepts*, its definition of integration.

Governance to support the ability of the IDS member organizations to be *locally responsive* might have these characteristics:

- A small, central IT group is created to assist in local IT plan development; develop technical, data, and application standards; and perform technical research and development. This group has an advisory and coordination relationship with the local IT organizations.
- Local IT steering committees develop local IT plans according to processes and criteria defined locally. A central IT steering committee with an advisory role reviews these plans to identify and advise on areas of potential redundancy or serious inconsistency.
- IT budgets are developed locally according to overall budget guidelines established centrally—for example, there are rules for capitalizing new systems and selecting the duration to use for depreciation.
- Certain pieces of data are standardized to ensure that the IDS can prepare consolidated financial statements and patient activity counts.
- Local sites are free to, for example, select any e-mail system, but that system must be able to send and receive messages using Internet protocols and the local e-mail system directory must be accessible to other e-mail directories.

This approach reflects a strategy of ensuring that each IDS member has the latitude to respond to local market needs. This approach also reflects a governing concept in the form of a definition of integration. Each of the examples we have just given offers a different definition of integration, and both definitions are correct. As a result of these different definitions, IT governance will be different in these organizations, and both approaches to governance are correct.

IT governance structures and approaches must be designed so that they further organization goals and strategies. They should not be brought into existence purely to perform some normative task. For example, the thinking that says, “all organizations have IT steering committees composed of a broad representation of senior leadership

and hence so should we,” is misguided. If the organization has, for example, an objective of being locally responsive that may mean that no central steering committee should exist or that its powers should be limited.

IT, User, and Senior Management Responsibilities

Effective application of IT involves the thoughtful distribution of IT responsibilities between the IT department, users of applications and IT services, and senior management. In general these responsibilities address decision-making rights and roles. Although different organizations will arrive at different distributions of these responsibilities, and an organization’s distribution may change over time, there is a fairly normative distribution (Applegate, Austin, & McFarlan, 2003).

IT Department Responsibilities. The IT department should be responsible for the following:

- Developing and managing the long-term architectural plan and ensuring that IT projects conform to that plan.
- Developing a process to establish, maintain and evolve IT standards in several areas:
 - Telecommunications protocols and platforms
 - Client devices, e.g., workstations and PDAs, and client software configurations
 - Server technologies, middleware and database management systems
 - Programming languages
 - IT documentation procedures, formats and revision policies
 - Data definitions (this responsibility is generally shared with the organization function, e.g., finance and health information management, that manages the integrity and meaning of the data)
 - IT disaster and recovery plans
 - IT security policies and incident response procedures
- Developing procedures that enable the assessment of sourcing options for new initiatives, e.g., build vs. buy new applications or leveraging existing vendor partner offerings versus utilizing a new vendor when making an application purchase
- Maintaining an inventory of installed and planned systems and services and developing plans for the maintenance of systems or the planned obsolescence of applications and platforms
- Managing the professional growth and development of the IT staff
- Establishing communication mechanisms that help the organization understand the IT agenda, challenges and services and new opportunities to apply IT
- Maintaining effective relationships with preferred IT suppliers of products and services [Applegate, Austin, & McFarlan, 2003].

The scope and depth of these responsibilities may vary. Some of the responsibilities of the IT group may be delegated to others. For example, some non-IT departments may be permitted to have their own IT staff and manage their own systems. This should be done only with the approval of senior management. And the IT department should be asked to provide oversight of the departmental IT group to ensure that professional standards are maintained and that no activities that compromise the organization's systems are undertaken. For example, the IT department can ensure that virus control procedures and software are effectively applied.

The organization may decide that the IT department should have almost imperial authority in carrying out its responsibilities or that its role should be closer to adviser to senior management. Organizations generally arrive at a level of authority in between imperial and advisory—a level based on experience and recent history.

In general, the IT department is responsible for making sure that both individual and organizational information systems are reliable, secure, efficient, current, and supportable. It is also usually responsible for managing the relationship with suppliers of IT products and services and ensuring that the processes that lead to new IT purchases are rigorous.

User Responsibilities. IT users (primarily middle management and supervisors) have several IT-related responsibilities:

- Understanding the scope and quality of IT activities that are supporting their area or function
- Ensuring that the goals of IT initiatives reflect an accurate assessment of the function's needs and challenges and that the estimates of the function's resources (personnel time, funds and management attention) needed by IT initiatives, e.g., to support the implementation of a new system, are realistic
- Developing and reviewing specifications for IT projects and ensuring that ongoing feedback are provided to the IT organization on implementation issues, application enhancements and IT support, e.g., ensuring that the new application has the functionality needed by the user department
- Ensuring that the applications used by a department are functioning properly, e.g., by periodically testing the accuracy of system-generated reports and checking that passwords are deleted when staff leave the organization
- Participating in developing and maintaining the IT agenda and priorities [Applegate, Austin, & McFarlan, 2003]

These responsibilities constitute a minimal set. In Chapter Seven, we discussed an additional, and more significant, set of responsibilities during the implementation of new applications.

Senior Management Responsibilities. The primary IT responsibilities of the senior leadership are as follows:

- Ensuring that the organization has a comprehensive, thoughtful and flexible IT strategy
- Ensuring an appropriate balance between the perspectives and agendas of the IT organization and the users, e.g., the IT organization may want a new application that has the most advanced technology while the user department wants the application that has been used in the industry for a long time
- Establishing standard processes for budgeting, acquiring, implementing and supporting IT applications and infrastructure
- Ensuring that IT purchases and supplier relationships conform to organizational policies and practices, e.g., contracts with IT vendors need to use standard organizational contract language
- Developing, modifying and enforcing the responsibilities and roles of the IT organization and users
- Ensuring that the IT applications and activities conform to all relevant regulations and required management controls and risk mitigation processes and procedures
- Encouraging the thoughtful review of new IT opportunities and appropriate IT experimentation [Applegate, Austin, & McFarlan, 2003]

Perspective: Principles for IT Investments and Management

Charlie Feld and Donna Stoddard have identified three principles for effective IT investments and management. They note that the responsibility for developing and implementing these principles lies with the organization's senior leadership.

1. *A long-term IT renewal plan linked to corporate strategy.* Organizations need IT plans that are focused on achieving the organization's overall strategy and goals. The organization must develop this IT renewal plan and remain focused, often over the course of many years, on its execution.
2. *A simplified, unifying corporate technology platform.* This IT platform must be well architected and be defined and developed from the perspective of the overall organization rather than the accumulation of the perspectives of multiple departments and functions.
3. *A highly functional, performance-oriented IT organization.* The IT organization must be skilled, experienced, organized, goal-directed, responsive, and continuously work on establishing great working relationships with the rest of the organization.

Feld and Stoddard (2004)

Although organizations will vary in the ways they distribute decision-making responsibility and roles and the ways in which they implement them, problems may arise when the distribution between groups is markedly skewed (Applegate, Austin, & McFarlan, 2003).

Too much user responsibility can lead to a series of uncoordinated and under-managed user investments in information technology. This occurs when a number of independent user departments make IT decisions that result in a wide range of technologies and vendors, making it difficult to manage and integrate these systems. Users can also underestimate the difficulty of managing IT platforms and make poor technology decisions. This can result in

- An inability to achieve integration between highly heterogeneous systems
- Insufficient attention to infrastructure, resulting in application instability
- High IT costs, due to insufficient economies of scale, significant levels of redundant activity, and the cost of supporting a high number of heterogeneous systems
- A failure to leverage IT opportunities because of user ignorance or fear of IT—for example, users won't invest in needed applications because they are afraid to do so
- A lack of, or uneven, rigor applied to the assessment of the value of IT initiatives—for example, insufficient homework may be done and an application selected that has serious functional limitations

Too much IT responsibility can lead to

- Too much emphasis on technology, to the detriment of the fit of an application with the user function's need—for example, when a promising application does not completely satisfy the IT department's technical standards, IT will not allow its acquisition
- A failure to achieve the value of an application due to user resistance to a solution imposed by IT: "We in the IT department have decided that we know what you need. We don't trust your ability to make an intelligent decision."
- Too much rigor applied to IT investment decisions; excessive bureaucracy can stifle innovation
- Very high proportion of the IT budget devoted to infrastructure, to the detriment of application initiatives, as the IT department seeks to achieve ever greater levels (although perhaps not necessary levels) of reliability, security, and agility
- Reduction in business innovation when IT is unwilling to experiment with new technologies that might have stability and supportability problems

Either extreme can clearly create problems. And no compromise position will make the IT department and the IT users happy with all facets of the outcome. An

outcome of “the best answer we can develop but not an answer that satisfies all” is an inevitable result of the leadership discussion of responsibility and role distribution.

Specific Governance Structures

In any organization there may be a plethora of committees and a series of complex reporting relationships and accountabilities, all of which need to operate with a fair degree of harmony in order for governance to be effective. Among them should be five core *structures* for governing IT:

1. Board responsibility for IT.
2. A senior leadership forum that guides the development of the IT agenda, finalizes the IT budget, develops major IT-centric policies, and addresses any significant IT issue that cannot be resolved elsewhere. This core structure includes subcommittees, designated by the forum, that have specific roles and responsibilities—for example, a privacy committee might be formed or a care improvement committee that is charged with overseeing the implementation of a clinical information system.
3. Initiative- and project-specific committees and roles (this structure will be discussed in Chapter Fourteen)
4. IT liaison relationships
5. The chief information officer (CIO) and other IT staff (described in Chapter Eleven)

The Board. The health care organization’s board holds the fundamental accountability for the performance of the organization, including the IT function. The board must decide how it will carry out its responsibility with respect to IT.

At a minimum this responsibility involves receiving a periodic update (perhaps annually), at a board meeting, from the CIO about the status of the IT agenda and the issues confronting the effective use of IT. In addition, financial information systems controls and IT risk mitigation are often identified and discussed by the board’s audit committee and the IT budget is discussed by the finance committee.

Some organizations create an IT committee of the board. Realizing that the normal board agenda might not always allow sufficient time for discussion of important IT issues and that not all board members have deep experience in IT, the board can appoint a committee of board members who are seasoned IT professionals (IT academics, CIOs of regional organizations, and leaders in the IT industry). The committee, chaired by a trustee, need not be composed entirely of board members. IT professionals who are not on the board may serve as members too. This committee informs the board of its assessments of a wide range of IT challenges and initiatives and makes recommendations about these issues.

The charter for such a committee might charge the committee to

- Review and critique IT application, technical, and organization strategies
- Review and critique overall IT tactical plans and budgets
- Discuss and provide advice on major IT issues and challenges
- Explore opportunities to leverage vendor partnerships

Committee meeting agenda items might include

- Assessments of the value of clinical information systems
- Long-term plans for the organization's financial systems
- IT staff recruitment and retention issues
- The annual IT budget

The leadership of an organization should not believe, however, that appointing an IT committee gets the board off the hook for having to deal with IT issues. Rather, this committee should be viewed as a way for all board members to continue their efforts to become more knowledgeable and comfortable with the IT conversation.

Senior Leadership Organizational Forum. Most health care organizations have a committee called something like the *executive committee*. This committee is composed of the senior leadership of the organization and is the forum in which strategy discussions occur and major decisions regarding operations, budgets, and initiatives are made. It is highly desirable to have the CIO as a member of this committee.

Major IT decisions should be made at the meetings of this committee. These decisions will cover a gamut of topics, such as approving the outcome of a major system selection process, defining changes in direction that may be needed during the course of significant implementations, setting IT budget targets, and ratifying the IT component of the strategic planning efforts.

This role does not preclude the executive committee from assigning IT-related tasks or discussions to other committees. For example, a medical staff leadership committee may be asked to develop policies regarding physician use of computerized provider order entry. A committee of department heads may be asked to select a new application to support registration and scheduling. A committee of human resource staff may be charged with developing policies regarding organizational staff use of the Internet while at work.

The executive committee, major departments and functions, and several high-level committees will regularly be confronted with IT topics and issues that did not arise from the organization's IT plan and agenda. For example, a board member may ask if the organization should outsource its IT function. Several influential physicians

may suggest that the organization assess a new information technology that seems to be getting a lot of hype. The CEO may ask how the organization should (or whether it should) respond to an external event—for example, a new Institute of Medicine report. The organization may need to address new regulations—for example, rules devolving from the Health Insurance Portability and Accountability Act (HIPAA).

When it is not clear which person or committee should address these issues or topics, they could be brought forth during an executive committee meeting for triage. (Alternatively, the CEO, CFO, CIO, or COO may decide where an issue should be handled.) The executive committee can form a task force to examine the issue and develop recommendations, or it can request that an existing forum or function address the issue. For example, a task force of clinicians and IT staff could be asked to examine the ramifications of a new Institute of Medicine report. The organization's legal department could be charged with developing the organization's response to new legislation.

Some organizations create an IT steering committee and charge this committee with addressing all IT issues and decisions. The use of such committees is uneven in health care organizations. Approximately half have such a committee, and most of these committees are not regarded as functioning effectively.

If an organization has an IT steering committee that works well, it should leave it alone. In general, however, such committees are not a good idea. They tend not to be composed of the most senior leadership, and hence their links to the thinking process of the CEO and the executive committee are not strong. They tend to view IT issues in isolation from the overall issues facing the organization, and few IT issues can be dealt with well in isolation. And committee members often wind up fighting each other over parochial slices of the pie during the IT budget discussion.

IT steering committees are often seen as a senior leadership effort to get "IT problems" off their plate and onto someone else's plate. This is an abdication of responsibility.

IT Liaison Relationships. All major functions and departments of the organization—for example, finance, human resources, member services, medical staff affairs, and nursing—should have an IT liaison. The IT liaison is responsible for

- Developing effective working relationships with the leadership of each major function
- Ensuring that the IT issues and needs of these functions are understood and communicated to the IT department and the executive committee
- Working with function leadership to ensure appropriate IT representation on function tasks forces and committees that are addressing initiatives that will require IT support
- Ensuring that the organization's IT strategy, plans and policies, and procedures are discussed with function leadership

The IT liaison role is an invaluable one. It ensures that the IT department and the IT strategy receive needed feedback and that function leaders understand the directions and challenges of the IT agenda. It also promotes an effective collaboration between IT and the other functions and departments.

Perspective: Improving Coordination and Working Relationships

Carol Brown and Vallabh Sambamurthy have identified five mechanisms used by IT groups to improve their coordination and working relationships with the rest of the organization.

1. *Integrators* are individuals who are responsible for linking a particular organization department or function with the IT department. An integrator might be a CIO who is a participant in senior management forums. An integrator might also be an IT person who is responsible for working with the finance department on IT initiatives that are centered on that function; such a person might have a title such as *manager, financial information systems*.
2. *Groups* are committees and task forces that regularly bring IT staff and organization staff together to work collectively on IT issues. These groups could include, for example, the information systems steering committee or a standing joint meeting between IT and nursing to address current IT issues and review the status of ongoing IT initiatives.
3. *Processes* are organizational approaches to management activity such as developing the IT budget, selecting new applications, and implementing new systems. These processes invariably involve both IT and non-IT staff.
4. *Informal relationship building* includes a series of activities such as one-on-one meetings, IT staff presentations at department head meetings, and co-location of IT staff and user staff.
5. *Human resource practices* include training IT staff on team building, offering user feedback to IT staff during their reviews, and having IT staff spend time in a user area observing work.

Brown and Sambamurthy, 1999

Variations. The specific governance structures just described are typical in medium-sized and large provider or payer organizations. In other types of health care settings these structures will be different.

A medium-sized physician group might not have a separate board. The physicians and practice manager may be both the board and the senior leadership forum. The group might not need a CIO. Instead the practice administrator may manage contracts and relationships with companies that provide practice management systems

and support workstations and printers. The practice administrator also may perform all user liaison functions.

A division within a state department of public health would not have a board, but it should have a forum where division leadership can discuss IT issues. IT decisions might be made there or at meetings of the leadership of the overall department. Similarly, the CIO for the department may not have organized IT in a way that results in a division CIO. And the staff of the department CIO may provide user liaison functions for the division.

Despite these variations, effective management of IT requires

- A senior management forum where major IT decisions are made
- A person responsible for day-to-day management of the IT function and for ensuring that an IT strategy exists
- Mechanisms for ensuring that IT relationships have been established with major organization functions

In addition, although the structures will vary, the guidance for the respective roles of IT, users, and management remains the same. The desirable attributes of the person responsible for IT are unchanged. And the properties of good governance do not change.

Perspective: Archetypes of IT Governance Decision Making

Peter Weill and Jeanne Ross have identified six basic archetypes of IT governance. Each archetype describes an approach to making major IT decisions.

1. *Business monarchy*: a group of business executives, often an executive committee; may include the CIO
2. *IT Monarchy*: a group of IT executives or the CIO individually
3. *Feudal*: a committee of business unit leaders or key process owners
4. *Federal*: a committee of senior leadership and business unit leaders; may include IT leadership and senior managers
5. *IT duopoly*: IT executives and one other group—for example, IT leadership and finance leadership
6. *Anarchy*: each individual or business unit on its own

Any one health care organization may have several of these forms of governance but apply them in different areas. For example, a business monarchy may decide IT strategy but an IT monarchy may be used to establish architecture standards. In addition, an IT duopoly may be asked to select and implement a new revenue management system.

Weill and Ross, 2004

Organizational Effectiveness in IT

Several studies have examined organizations that have been particularly effective in the use of IT. Determining effectiveness is difficult, and these studies have defined organizations that show effectiveness in IT in a variety of ways. Among them are organizations that have developed information systems that defined an industry—as Amazon.com has altered the retail industry, for example—organizations that have a reputation for being effective over decades, and organizations that have demonstrated exceptional IT innovation.

The studies have attempted to identify those organizational factors or attributes that have led to or created the environment in which effectiveness has occurred. In effect the studies have sought to answer the question, What are the organizational factors that result in some organizations developing truly remarkable IT prowess?

If an organization understands these attributes and desires to be very effective in its use of IT, then it is in a position to develop strategies and approaches to create or modify its own attributes. For example, one attribute is strong working relationships between the IT function and the rest of the organization. If an organization finds that its own relationships are weak or dysfunctional, strategies and plans can be created to improve them.

The studies suggest that organizations that aspire to high levels of effectiveness and innovation in their application of IT must take steps to ensure that the core capacity of the organization to achieve such effectiveness is developed. It is a critical IT responsibility of organizational leadership to continuously (year in and year out) identify and effect steps needed to improve overall effectiveness in IT. The development of this capacity is a challenge different from the challenge of identifying specific opportunities to use IT in the course of improving operations or enhancing management decision making. For an analogy, consider running. A runner's training, injury management, and diet are designed to ensure the core capacity to run a marathon. This capacity development is different from developing an approach to running a specific marathon, which must consider the nature of the course, the competing runners, and the weather.

Although having somewhat different conclusions (resulting in part from somewhat different study questions), the studies have much in common regarding capacity development. Four of these studies are summarized in the following sections.

Factors Leading to Visionary IT Applications

The Financial Executives Research Foundation sponsored a study, conducted by Sambamurthy and Zmud (1996), to identify factors that have led to the development of visionary IT applications. Visionary applications are “applications that help

managers make decisions, introduce new products and services more quickly and frequently, improve customer relations, and enhance the manufacturing process. Visionary IT applications seek to transform some of a firm's business processes in 'frame breaking' ways. These applications create a variety of benefits to businesses that not only affect their current operations but also provide opportunities for new markets, strategies and relationships" (p. 1).

The study had several findings:

The nature of visionary applications. Visionary applications focused on one or more of these activities: leveraging core business operations, enhancing decision making, improving customer service, or speeding up the delivery of new products and services. These applications were *platforms* that enabled the business to handle multiple work processes. An example of such a platform in health care is the electronic medical record (EMR) system.

Roles associated with visionary projects. Visionary projects required the participation of four key players. Envisioners conceptualized the initial ideas for a project. Project champions were instrumental in selling the envisioner's idea and its value to senior executives. Executive sponsors acted as champions, with seed funding and political support. IT experts supplied the necessary technical vision and expertise to ensure that the idea would work.

Ways to facilitate investment in visionary IT applications. Several factors facilitated investment in visionary applications:

- A climate existed that enabled employees to have the power, and the support, to undertake visionary applications that often carried significant personal and organizational risk.
- Mechanisms existed for investing continuously in the IT infrastructure.
- Coordinating mechanisms were established to bring together envisioners, project champions, executive sponsors, and IT experts.
- The role of the CIO, in addition to that of envisioner and IT expert, was to ensure that envisioners' proposals furthered the interests of the business, to be an architect and advocate for the corporate IT infrastructure, and to serve as the architect of IT-related coordinating mechanisms.

Rationale for justifying visionary IT applications. Visionary IT applications were generally defended using one of two distinct strategies: their contribution to critical work processes or their support of a primary strategic driver. In addition to the discussion and analyses that surrounded the selected strategy, prototypes, best-practice visits to other organizations, and consultants were often used to further organizational understanding of the proposed initiative.

Factors Producing Long-Term Competitiveness in IT Applications

Ross, Beath, and Goodhue (1996) examined those factors that enable organizations to achieve long-term competitiveness in the application of IT. This study identified the development and management of three key IT assets as being critical to achieving a sustained IT-based competitive advantage:

The IT human resource asset. A well-developed, highly competent IT human resource asset was one that “consistently solves business problems and addresses business opportunities through information technology.” This asset had three dimensions:

1. IT staff had the technical skills needed to craft and support applications and infrastructures and to understand and appropriately apply new technologies.
2. IT staff had superior working relationships with the end-user community and were effective at furthering their own understanding of the business: its directions, cultures, work processes, and politics.
3. IT staff were responsible, and knew that they were responsible, for solving business problems. This orientation went beyond performing discreet tasks and led IT staff to believe that they “owned” the challenge of solving business problems and had the power to carry out that ownership.

The technology asset. The technology asset consists of “sharable technical platforms and databases.” An effective technology asset had two distinguishing characteristics:

1. A well-developed technology architecture
2. Standards that limited the variety of technologies that would be supported

Failure to create a robust architecture can result in applications that are difficult to change, not integrated, expensive to manage, and resistant to scaling (Weill & Broadbent, 1998). These limitations hinder the ability of the organization to advance. IT resources, efforts, and capital can be consumed by the difficulty of managing the current base of infrastructure, and applications and relatively modest advances can be too draining.

The relationship asset. When the relationship asset was strong, IT and each business unit’s management shared the risk and responsibility for effective application of IT in the organization. A solid relationship asset was present when the business unit was the owner, and was accountable for, all unit IT projects, and top management led the IT priority-setting process.

This study also noted the interrelationships between the assets. IT and user relationships were strengthened by the presence of a strong IT staff. A well-developed,

agile infrastructure enabled the IT staff to execute project delivery at high levels and be more effective at solving business problems.

Factors Leading to the Creation of Industry Changing Information Systems

McKenney, Copeland, and Mason (1995) studied those factors that resulted in successful managerial teams' creating and implementing innovative information systems. They were particularly interested in those examples where the resulting information systems became the dominant design in a particular industry. They studied American Airlines, Bank of America, United States Automobile Association, Baxter Travenol/American Hospital Association, and Frito-Lay. Their study generated several conclusions:

Management team. IT innovations were led proactively by a management team driven to change its processes through the means of IT. The management team had to play three essential roles:

1. The CEO or other senior executive was both visionary and a good business person. This person had sufficient power and prestige to drive technological innovation.
2. A technology maestro, often the CIO, had a remarkable combination of business acumen and technological competence. The CIO had to deliver the system and had to recruit, energize, and lead a superb technical team.
3. The technical team understood how to apply the technology in innovative ways and was capable of developing new business processes that leveraged the technology.

In addition to exceptional competence in each role, in the companies studied there was a rare chemistry between the players in the roles. A change in a role's incumbent often stalled the innovation. This suggests that a great CIO in one setting may not be a great CIO in another setting.

Evolution of the innovation. Innovative systems evolved over time and generally went through several phases of evolution:

- A business crisis developed—Bank of America for example, was overwhelmed by the volume of paper transactions—and a search began for an IT solution.
- IT competence was built as necessary research and development was done for potential IT solutions, particularly the application of emerging technologies.
- The IT solution was planned and developed.
- IT was used to restructure the organization and its processes and to lead changes in organization strategies.
- The strategy evolved and the systems were refined. Competitors began to emulate the success.

Throughout these phases the capabilities of the technology heavily influenced and constrained the operational changes that were envisioned and implemented. This series of phases occurred over five to seven years, reflecting the magnitude of the organizational change and the time required to experiment with, understand, and implement new information technology at scale. This interval suggests that a CIO (or CEO) average tenure of three years or less risks hindering the organization's ability to make truly innovative, IT-based transformations.

Capitalizing on IT innovation. A particular IT innovation was identified by the organization early in the life of the technology as being the breakthrough necessary to resolve a business crisis or challenge. Across the cases studied the breakthroughs were the transistor, time-sharing, and cheap mass storage. Today a breakthrough technology might be the Internet or voice recognition.

Factors That Increase the Value Received from IT Investments

Weill and Broadbent (1998) studied firms that “consistently achieve more business value for their information technology investment.” This study noted that these organizations were excellent or above average in five characteristics:

Commitment to the strategic and effective application of IT. This commitment was widely known within the organization. Management participated actively in IT strategy discussions, thoughtfully assessed the business contribution of proposed IT investments, and provided seed funding to innovative and experimental IT projects.

Less political turbulence. IT investments often served to integrate processes and groups across the organization. Political conflict reduced the likelihood and the success of interdisciplinary initiatives. IT investments can require that proposals for one part of the organization be funded at the expense of other parts or of proposed non-IT initiatives. Political turbulence can reduce the likelihood that such “disproportionate” investments will occur.

More satisfied users. When organizational staff had had good experiences with IT projects, they were more likely to view IT as something that could assist their endeavors, rather than as a burden or a function that was anchoring the organization to one spot.

Integrated business information technology planning. Organizations that did a very good job of aligning IT plans and strategies with overall organizational plans and strategies were more effective with IT than those that did not align well.

More experience. Organizations that were experienced in their use and application of the technology, and had had success in those experiences, were more thoughtful and focused in their continued application of IT. They had a better understanding of the technology's capabilities and limitations. Users and their IT colleagues had a better understanding of their respective needs and roles and the most effective ways of working together on initiatives.

Summary of Studies

The studies discussed in the preceding pages suggest that organizations that aspire to effectiveness and innovation in their application of IT must take steps to ensure that their core capacity for IT effectiveness is developed to the point where high levels of progress can be achieved and sustained. The development of this capacity is a challenge different from the task of identifying specific opportunities to use IT in the course of improving core processes or ensuring that the IT agenda is aligned with the organizational agenda.

Although having somewhat different conclusions, the four studies have much in common when they consider capacity development:

Individuals and leadership matter. It is critical that the organization possess talented, skilled, and experienced individuals. These individuals will occupy a variety of roles: CEO, CIO, IT staff, and user middle management. These individuals must be strong contributors. Although such an observation may seem trite, too often organizations, dazzled by the technology or the glorified experiences of others, embark on technology crusades and substantive investments that they have insufficient talent or leadership to effect well. The studies found that leadership is essential. It is an essential trait of the organization's senior management (or executive sponsors), the CIO, and the project team. Leaders must understand the vision, communicate the vision, be able to recruit and motivate a team, and have the staying power to see the innovation through several years of work with disappointments, setbacks, and political problems along the way.

Relationships are critical. Not only must the individual players be strong, the team must be strong. There are critical senior executive, IT executive, and project team roles that must be filled by highly competent individuals, *and* great chemistry must exist between the individuals in these distinct roles. Substitutions among team members, even when involving a replacement by an equally strong individual, can diminish the team. This is as true in IT innovation as it is in sports. Political turbulence diminishes the ability to develop a healthy set of relationships among organizational players.

The technology and technical infrastructure enables and hinders. New technologies can provide new opportunities for organizations to embark on major transformations of their activities. This implies that the health care CIO must have not only superior business and clinical understanding but also superior understanding of the technology. This should not imply that CIOs must be able to rewrite operating systems as well as the best system programmers, but it does mean that they must have superior understanding of the maturity, capabilities, and possible evolutions of various information technologies. Several innovations have occurred because an IT group was able to identify and adopt an emerging technology that could make a significant contribution to addressing a current organizational challenge. The studies also stress the importance of well-developed technical architecture. Great architecture matters. Possessing state of the art technology can be far less important than a well-architected infrastructure.

The organization must encourage innovation. The organization's (and the IT department's) culture and leadership must encourage innovation and experimentation. This encouragement needs to be practical and goal directed: a real business problem, crisis, or opportunity must exist, and the project must have budgets, political protection, and deliverables.

True innovation takes time. Creating visionary applications or industry dominant designs or an exceptional IT asset takes time and a lot of work. In the organizations studied by McKenney, Copeland, and Mason (1995), it often took five to seven years for the innovation to fully mature and for the organization to recast itself. Applications and designs will proceed through phases that are as normative as the passage from being a child to being an adult. Innovation, like the maturation of a human being, will see some variations in timing, depth, and success at moving through phases.

Evaluation of IT opportunities must be thoughtful. Visionary and dominant-design IT innovations should be analyzed and studied thoroughly. Nonetheless, organizations engaged in these innovations should also understand that a large amount of vision, management instinct, and "feel" guides the decision to initiate investment and continue investment. The organization that has had more experiences with IT, and more successful experiences, will be more effective in the evaluation (and execution) of IT initiatives.

Processes, data, and differentiation form the basis of an IT innovation. All the innovations studied were launched from management's fundamental understanding of current organizational limitations. Innovations should focus on the core elements discussed in Chapter Twelve as the basis for achieving an IT-based advantage: significant leveraging of processes, expanding and capitalizing on the ability to gather critical data, and achieving a high level of organizational differentiation. Often an organization can pursue all three simultaneously. At other times an organization may evolve from one basis to another as the competition responds or as it sees new leverage points.

Alignment must be mature and strong. The alignment between the IT activities and the business challenges or opportunities must be strong. It should also be mature in the sense that it depends on close working relationships rather than methodologies.

The IT asset is critical. Strong IT staff, well-designed IT governance, well-crafted architecture, and a superb CIO are critical contributors to success. There is substantial overlap between the factors identified in these studies and the components of the IT asset.

Perspective: Principles for High Performance

Robert Dvorak, Endre Holen, David Mark, and William Meehan have identified six principles at work in a high-performance IT function:

1. IT is a business-driven line activity and not a technology-driven IT staff function. Non-IT managers are responsible for selecting, implementing, and realizing the benefits of new applications. IT managers are responsible for providing cost-effective infrastructure to enable the applications.
2. IT funding decisions are made on the basis of value. Funding decisions require thorough business cases. IT decisions are based on business judgment and not technology judgment.
3. The IT environment emphasizes simplicity and flexibility. IT standards are centrally determined and enforced. Technology choices are conservative and packaged applications are used wherever possible.
4. IT investments have to deliver near-term business results. The 80/20 rule is followed for applications, and projects are monitored relentlessly against milestones.
5. The IT operation engages in year-to-year operation productivity improvements.
6. A business-smart IT function and an IT-smart business organization are created. Senior leadership is involved in and conversant with IT decisions. IT managers spend time developing an understanding of the business.

Dvorak, Holen, Mark, and Meehan, 1997

The Senior Leader in the Information Age

Earl and Feeney (2000) assessed the characteristics and behaviors of senior leaders (in this case CEOs) who were actively engaged and successful in the strategic use of IT. These leaders were convinced that IT could and would change the organization. They placed the IT discussion high on the strategic agenda. They looked to IT to identify opportunities to make significant improvements in organizational performance, rather than viewing the IT agenda as secondary to strategy development. They devoted personal time to understanding how their industry and their organization would evolve as IT evolved. And they encouraged other members of the leadership team to do the same.

Earl and Feeney (2000) observed five management behaviors in these leaders:

1. *They studied rather than avoided IT.* They devoted time to learning about new technologies and, through discussion and introspection, developed an understanding of the ways in which new technologies might alter organization strategies and operations.
2. *They incorporated IT into their vision of the future* of the organization and discussed the role of IT when communicating that vision.
3. *They actively engaged in IT architecture discussions and high-level decisions.* They took time to evaluate major new IT proposals and their implications. They were visibly supportive of architecture standards. They established funds for the exploration of promising new technologies.

4. *They made sure that IT was closely linked to core management processes:*

They integrated the IT discussion tightly into the overall strategy development process. This often involved setting up teams to examine aspects of the strategy and having both IT and business leaders at the table.

They made sure IT investments were evaluated as one component of the total investment needed by a strategy. The IT investments were not relegated to a separate discussion.

They ensured strong business sponsorship for all IT investments. Business sponsors were accountable for managing the IT initiatives and ensuring the success of the undertaking.

5. *They continually pressured the IT department to improve its efficiency and effectiveness and to be visionary in its thinking.*

CEOs and other members of the leadership team have an extraordinary impact on the tone, values, and direction of an organization. Hence their beliefs and daily behaviors have a significant impact on how effectively and strategically information technology is applied within an organization.

IT Budget

Developing budgets is one of the most critical management undertakings. The budget process forces management to make choices between initiatives and investments and requires analysis of the scope and impact of any initiative—for example, it answers questions such as, Will this initiative enable us to reduce supply costs by 3 percent?

Developing the IT budget is challenging, for several reasons:

- The IT projects proposed at any one time are eclectic and thus difficult to compare. In addition to the IT initiatives proposed as a result of the alignment and strategic planning process, other initiatives may be put forward by clinical or administrative departments that desire to improve some aspect of their performance. Also on the table may be IT projects designed to improve infrastructure—for example, a proposal to upgrade servers. These initiatives will all be different in character and in the return they offer, making them difficult to compare.
- Dozens, if not hundreds, of IT proposals may be made, making it challenging to really understand all the requests.
- The aggregate request for capital and operating budgets can be too expensive. It is not unusual for requests to total three to four times more money than the organization can afford. Even if it wanted to fund all of the requests, the organization doesn't have enough money to do so.

And yet the budget process requires that the organization grapple with these complexities and arrive at a budget answer.

Basic Budget Categories

To facilitate the development of the IT budget, the organization should develop some basic categories that organize the budget discussion.

Capital and Operating. The first category distinguishes between *capital* and *operating* budgets. Financial management courses are the best place to learn about these two categories. In brief, however, capital budgets are the funds associated with purchasing and deploying an asset. Common capital items in IT budgets are hardware and applications. Operating budgets are the funds associated with using and maintaining the asset. Common operating items in IT budgets are hardware maintenance contracts and the salaries of IT analysts. In an analogous fashion, the purchase of a car is a capital expense. Gasoline and tune-ups are operating expenses. Both capital and operating budgets are prepared for IT initiatives.

Support, Ongoing, and New. *Support* refers to those IT costs (staff, hardware, and software licenses) necessary to support and maintain the applications and infrastructure that are in place now. Software maintenance contracts ensure that applications receive appropriate upgrades and bug fixes. Staff are needed to run the computer rooms and perform minor enhancements. Disk drives may need to be replaced. Failure to fund support activities can make it much more difficult to ensure the reliability of systems or to evolve applications to accommodate ongoing needs—for example, adding a new test to the dictionary for a laboratory system or introducing a new plan type into the patient accounting system.

Ongoing projects are those application implementations begun in a prior year and still under way. The implementation of a patient accounting system or a computerized provider order entry system can take several years. Hence a capital and operating budget is needed for several years to continue the implementation.

New projects are just that—there is a proposal for a new application or infrastructure application. The IT strategy may call for new systems to support nursing. Concerns over network security may lead to requests for new software to deter the efforts of hackers.

Support Current Operations or Strategic Plan. Proposals may be directed to supporting current operations, perhaps by responding to new regulations or streamlining the workflow in a department. Proposals may also be explicitly linked to an aspect of

the health care organization’s strategic plan—they might call for applications to support a strategic emphasis on disease management, for example.

Budget Targets. During the budget process, organizations define targets for the budget overall and for its components. For example, the organization might state that it would like to keep the overall growth in its operating budget to 2 percent but is willing to allow 5 percent growth in the IT operating budget. The organization might also direct that within that overall 5 percent growth, the budget for support should not grow by more than 3 percent but the budget for new projects and ongoing projects combined can grow by 11 percent. Table 13.1 illustrates the application of overall and selective operating budget targets.

Similarly, targets can be set for the capital budget. For example, perhaps it will be decided that the capital budget for support should remain flat but that given the decision to invest in an EMR, the overall capital budget will increase to accommodate the capital required by the EMR investment.

Management Development of IT Budget Categories

The management discussion of the IT budget begins with the discussion of its categories and targets. Should the organization develop categories such as support, ongoing, and new? Should it assign selective budget targets by category? What should those targets be? There are no rules for this conversation. There is no optimal outcome.

However, the categories can be used to achieve various objectives. On the one hand, support often accounts for 70 to 80 percent of the IT operating budget and 20 to 30 percent of its capital budget. The organization can decide that support must work well but is of modest strategic value. Hence the budget orientation is to be efficient with support. The budget target should be sufficient to cover salary growth and increases in maintenance contracts but it should also encourage ongoing efforts to be more efficient. Efficiency can be gained, for example, by asking the IT function every year to achieve a 2 percent improvement in efficiency. On the other hand, an IT

TABLE 13.1. TARGET INCREASES IN AN IT OPERATING BUDGET.

	Support Operations	Strategic Initiatives	Total
Ongoing and new	9%	15%	11%
Support	3%	3%	3%
TOTAL	4%	7%	5%

agenda with several important strategic initiatives may lead the organization to conclude that it will allow a 7 percent growth in the operating budget to support strategic initiatives but a more modest 4 percent growth in initiatives to support operations.

Whatever the outcome of the management discussion, the IT budget categories should remain consistent from year to year so that yearly comparisons of the budget can be made. Moreover, stability in definitions enables the management team to develop a common language and concepts during budget discussions. However, the targets may change annually depending on the fiscal health of the organization and the strategic importance of the IT agenda.

IT Budget Development

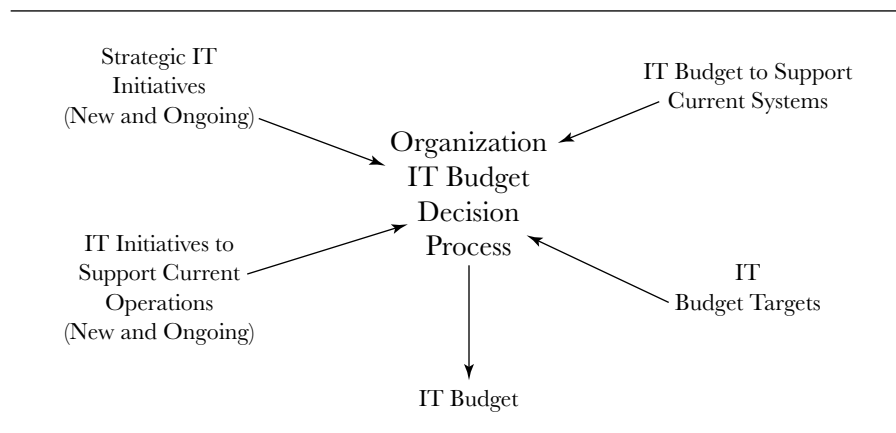
In addition to formulating the categories already discussed, organizational leadership will need to develop the process by which the IT budget is discussed, prioritized, and approved. In other words, it must answer the question, What processes will we use to decide which projects will be approved subject to our targets? An example of a budget process is outlined in this section and illustrated in Figure 13.1.

This process example has five components, and the steps described here use some typical targets.

First, the IT department submits an operating budget to support the applications and infrastructure that will be in place as of the beginning of the fiscal year (the support budget). This budget might be targeted to a 3 percent increase over the support budget for the prior fiscal year. The 3 percent increase reflects inflation, salary increases, a recognition that new systems were implemented during the fiscal year and will require support, and an acknowledgment that infrastructure (workstations, remote locations, and storage) consumption will increase. A figure for capital to support applications and infrastructure is also submitted, and it should be the same as that which was budgeted in the prior fiscal year. If the support operating and capital budgets achieve their targets, there is minimal management discussion of those budgets.

Second, IT leadership reviews the strategic IT initiatives (new and ongoing) with the senior leadership of the organization. This review may occur in a forum such as the executive committee. This committee, mindful of its targets, determines which strategic initiatives will be funded. If the budget being sought to support strategic IT initiatives is large or a major increase over the previous year, there will be discussions about the budget with the board.

Third, the organization must decide which new and ongoing initiatives that support current operations—for example, a new clinical laboratory or contract management system—will be funded. These discussions must occur in the forum where the overall operations budget is discussed. The forums in which such discussions occur are generally organizational meetings that routinely discuss operations and that number among

FIGURE 13.1. IT BUDGET DECISION-MAKING PROCESS.

their members the managers of major departments and functions. Budget requests for new IT applications are reviewed in the same conversation that discusses budget requests for new clinical services or improvement of the organization's physical plant.

Fourth, both the strategy budget discussion and the operations budget discussion follow a set of ground rules:

- The IT budget is discussed in the same conversations as are non-IT budget requests. This will result in trade-offs between IT expenditures and other expenditures. This integration forces the organization to examine where it believes its monies are best spent, asking, for example, Should we invest in this IT proposal or should we invest in hiring staff to expand a clinical service? Following this process also means that IT requests and other budget requests are treated no differently.
- The level of analytical rigor required of the IT projects is the same as that required of any other requested budget item.
- Where appropriate, a sponsor—for example, a clinical vice president or a CFO—defends the IT requests that support his or her department in front of his or her colleagues. The IT staff or CIO should be asked to defend infrastructure investments—for example, major changes to the network—but should not be asked to defend applications.

The ground rule that sponsors should present their own IT requests deserves a bit more discussion, because the issue of who defends the request has several important ramifications, particularly for initiatives designed to improve current operations. Having this ground rule has the following results:

It forces assessment of trade-offs between IT and non-IT investments. The sponsor will determine whether to present the IT proposal or some other, perhaps non-IT, proposal. The sponsor will decide whether the IT investment or another investment that he or she has reviewed should be made.

It forces accountability for investment results. The sponsor and his or her colleagues know that if the IT proposal is approved there will be less money available for other initiatives. The defender also knows that the value being promised must be delivered or his or her credibility in next year's budget discussion will be diminished.

It improves management comfort when dealing with IT proposals. The defender also learns how to be comfortable when presenting IT proposals.

It gets IT out of the role of defending other people's operation improvement initiatives. However, the IT function must still support the budget requests of others by providing data on the costs and capabilities of the proposed applications and the time frames and resources required to implement them. If the IT function believes that the proposed initiative lacks merit or is too risky, IT staff need to ensure that this opinion is heard during the budget approval process.

In the fifth and final step of the process, the operations and strategic budget recommendations are reviewed and discussed at an executive committee meeting. The executive committee can accept the recommendations, request further refinement (perhaps cuts) of the budget, or determine that a discussion of the budget is required at an upcoming board meeting.

Summary

The management and leadership of an organization play significant roles in determining the effectiveness of information technology. This chapter discussed the role of developing and maintaining IT governance mechanisms—the processes, procedures, and roles that the organization uses to make IT decisions. These decisions cover diverse terrain: budgets, roles, and responsibility distribution and the process for resolution of IT issues.

Health care executives must also take steps to improve the overall ability of the organization to apply IT. These steps may involve working on improving IT-user relationships, managing IT architecture, developing approaches to IT experimentation, ensuring IT strategic alignment, and developing the skills of the IT staff.

An annual responsibility of the leadership is determining the IT budget. Developing this budget is difficult. Comparing diverse and numerous IT proposals is challenging. However, the budget process can be made easier (although not easy) by establishing clear definitions of budget categories, category targets, and the process for IT proposal review.

Chapter Thirteen: Learning Activities

1. Interview a member of the senior leadership team of a health care organization on the subject of IT governance. Describe the organization's approach to IT governance, and assess its effectiveness.
2. Interview a health care CIO and a member of the senior leadership team of the same health care organization separately. Ask each of them to describe the process of preparing the IT budget. Compare and discuss their responses.
3. Interview a health care CIO and a member of the senior leadership team of the same health care organization separately. Ask each of them to describe the distribution of IT and user responsibilities. Compare and discuss their responses.
4. Assume that you are a consultant who has been asked to assess the effectiveness of an organization in applying IT. Construct a questionnaire (twenty questions) to guide the interviews of organizational leadership needed to determine effectiveness.



CHAPTER FOURTEEN

MANAGEMENT'S ROLE IN MAJOR IT INITIATIVES

Health care organizations routinely undertake projects or initiatives designed to improve the performance of the organization or advance its strategies through the use of new or existing information technologies. Many of these projects involve the implementation of a major application system and often these projects are labeled “IT projects.” Examples of such projects include implementing computerized provider order entry, streamlining the front-end processes of registration and scheduling, and enhancing the discharge process.

This chapter discusses the role of management in these IT projects. The strategy may have been defined and the IT agenda may have been aligned; now it is time to execute the plan. What role should management play during the execution of IT initiatives? What structures, processes, and roles should be in place to make sure that the initiatives are well managed?

This chapter covers three major topics:

- Managing organizational change due to IT initiatives
- Managing IT projects
- Understanding factors that contribute to IT initiative failures

Managing Organizational Change Due to IT Initiatives

A majority of IT initiatives involve or require organizational change—change in processes or organization structure or change in the form of expansion or contraction of roles or services. IT-enabled or IT-driven organizational change has several possible origins:

- The new IT system has capabilities different from those of the previous system and hence the workflow that surrounds the system has to change and the tasks that staff perform have to change. For example, if a new electronic medical record (EMR) system automatically generates letters for patients with normal test results, then the individuals who used to generate these letters will no longer have to do this task.
- The discussion surrounding the desired capabilities of a new application can lead to a reassessment of current processes, workflow, and distribution of tasks across staff and a decision to make changes in processes that extend well beyond the computer system. For example, the analysis surrounding a new patient accounting system might highlight problems that occur during registration and scheduling (such as failure to check insurance coverage during appointment check-in) that hinder the optimal performance of patient accounting. In this way a new system becomes a catalyst for a comprehensive set of changes.
- The health care organization's strategy may call for significant changes in the way the organization operates and delivers care. For example, the organization may decide to move aggressively to protocol-driven care. This transformation has extensive ramifications for processes, roles, and workflow and for the design of applications. New IT systems will be critical contributors to the changes needed, but they are not the epicenter of the change discussion.

Change management is an essential skill for the leaders of health care organizations. Although the need for this skill is not confined to situations that involve the implementation of major applications, change management is a facet of virtually all implementations of such applications.

Types of Organizational Change

Keen (1997) identified four categories of organizational change:

- Incremental
- Step-shift

- Radical
- Fundamental

Incremental Change. *Incremental* change occurs through a series (at times continuous) of small to medium-sized changes to processes, tasks, and roles. Each change carries relatively low risk, can be completed quickly, and is often accomplished without the need for substantial analysis or leadership intervention. At times, organizations establish an overall emphasis on continuous change and create groups to help departments make changes and measure change impact. Management movements such as Continuous Quality Improvement and Total Quality Management emphasize continuous, incremental change. Continuous, incremental change can be seen as plodding and lacking bold vision. However, this perception misses the power of such change over the course of time and the occurrence of such change across many facets of the organization. One should remember that the Grand Canyon was formed from continuous, incremental erosion.

The implementation of an application can involve change that is incremental. This is particularly true when the application is an upgrade of an existing application and has new reports and features that require modest alterations to existing workflow.

One outcome of continuous change may be the recognition that current application systems are progressively becoming a poor fit with the evolving organization. After several years of dealing with a growing gap between the capabilities of an application and the direction of an evolving organization, the organization may decide to purchase a new application; one that is a better fit.

Step-Shift Change. In *step-shift* change the leadership is committed to making significant changes but it is not changing the basic direction of the organization or how it generates value. Examples of such change include a focused effort to significantly reduce the cost of care or improve patient safety, the addition of a nonacute business line in an organization that has previously focused on acute care, and a major effort to improve the patient service experience in the outpatient clinics. Step-shift change involves an intense focus on a critical aspect of the organization and, for the areas within that focus, major changes in processes, roles, and tasks. Step-shift change is often driven by a strategic realization that the basis of competition has evolved to the point that in the absence of such change, the organization's success is in some degree of peril.

This type of change invariably leads to the implementation of major new applications. An emphasis on patient safety may lead to the implementation of computerized provider order entry, and an effort to improve the patient experience in outpatient care may result in the implementation of a new registration and scheduling application. At times the leadership responsible for implementing a new application will realize that this implementation creates the opportunity to effect step-shift

change, asking, for example, Why don't we take advantage of this new outpatient system to make significant improvements in the service experience?

Radical Change. *Radical* change leaves the organization and its core assumptions intact but significantly alters the way the organization carries out its business. The creation of an integrated delivery system from a collection of previously independent organizations is an example of radical change. The movement from fee-for-service reimbursement to full capitation (that is, fixed fee per patient per year) is radical change. Radical change always requires some changes, at times extensive changes, in the IT application portfolio. Because the way work is done has changed significantly across many facets of the organization, applications that fit the way work was previously done are no longer helpful.

In health care it is rare that IT will cause or lead to a decision to undergo radical organizational change. The Internet frenzy that occurred in the early part of this century led many health care organizations to wonder whether the Internet would *cause* radical change. For example, if patients could look up medical information on the Internet would this significantly reduce their need for physicians? This radical change did not occur, although use of the Internet has led to incremental and some step-shift change.

Fundamental Change. With *fundamental* change the leadership is committed to creating what will in effect be a new organization that is in a different business from the one the current organization engages in. Fundamental change has occurred for some companies. For example, the now deservedly much-maligned Enron changed its core business from acquiring and managing natural gas pipelines to managing a complex web of businesses that included a global broadband network and the trading of paper products. A health care example would be an acute care provider that closes all its beds and becomes a diagnostic imaging center. Fundamental change is risky, and the failure rate is very high.

Clearly, in these cases the entire IT application suite may need to be jettisoned and replaced with new applications that support the new business.

Effecting Organizational Change

The management strategies required to manage change depend on the type of change. As one moves from incremental to fundamental change, the magnitude and risk of the change increases enormously, as does the uncertainty about the form and success of the outcome.

In this section we will present some normative approaches to managing a blend of step-shift and radical change. Fundamental change is rare in health care. Incremental

change carries less risk and hence requires less management. Note, however, that a program of continuous incremental change is in effect a form of step-shift change.

Managing change of this magnitude (step-shift to radical) is deceptively simple and quite hard at the same time. It is the same duality encountered in raising children. At one level it is easy; all you have to do is feed, teach, protect, and love them. At another level, especially during the teenage years, it can be an exceptionally complicated, exasperating, and scary experience.

Managing change has several necessary aspects (Keen, 1997):

- Leadership
- Language and vision
- Connection and trust
- Incentives
- Planning, implementing, iterating

Leadership. Change must be led. Leadership, often in the form of a committee of leaders, will be necessary to

- Define the nature of the change
- Communicate the rationale and approach to the change
- Identify, procure, and deploy necessary resources
- Resolve issues, and alter direction as needed
- Monitor the progress of the change initiative

This leadership committee needs to be chaired by an appropriate senior leader. If the change affects the entire organization, the CEO should chair the committee. If the change is focused on a specific area, the most senior leader who oversees that area should chair the committee.

Language and Vision. The staff who are experiencing the change must understand the nature of the change. They must know what the world will look like (to the degree that this is clear) when the change has been completed, how their roles and work life will be different, and why making this change is important. The absence of this vision or a failure to communicate the importance of the vision elevates the risk that staff will resist the change and through subtle and not-so-subtle means cause the change to grind to a halt. Change is hard for people. They must understand the nature of the change and why they should go through with what they will experience as a difficult transition.

Leaders might describe the vision, the desired outcome of efforts to improve the outpatient service experience, in this way:

Patients should be able to get an appointment for a time that is most convenient for them.

Patients should not have to wait longer than ten minutes in the reception area before a provider can see them.

We should communicate clearly with patients about their disease and the treatment that we will provide.

We should seek to eliminate administrative and insurance busy work from the professional lives of our providers.

These examples illustrate a thoughtful use of language. They first and foremost focus on *patients*. But the organization also wants to improve the lives of its *providers*. The examples use the word *should* rather than the word *must* because it is thought that staff won't believe the organization can pull off 100 percent achievement of these goals and leaders don't want to establish goals seen as unrealistic. The examples also use the word *we* rather than words like *you*. *We* means that this vision will be achieved through a team effort, whereas *you* can imply that those hearing this message have to bear this challenge without leadership's help.

Connection and Trust. Achieving connection means that leadership takes every opportunity to present the vision throughout the organization. As a leader, you may use department head meetings, medical staff forums, one-on-one conversations in the hallway, internal publications, and e-mail to communicate the vision and to keep communicating the vision. Even when you start to feel ill because you have communicated the vision one thousand times, you have to communicate it another one thousand times. A lot of this communication has to be done in person, where others can see you, rather than hiding behind an e-mail. The communication must invite feedback, criticism, and challenges.

The members of the organization must trust the integrity, intelligence, compassion, and skill of the leadership. Trust is earned or lost by everything that you do or don't do as a leader. The members must also trust that you have thoughtfully come to the conclusion that the difficult change has excellent reasons behind it and represents the best option for the organization. Organizational members are willing to rise to a challenge, often to heroic levels, if they trust their leadership. Trust requires that you act in the best interests of the staff and the organization and that you listen and respond to the organization's concerns.

Incentives. Organizational members must be motivated to support significant change. At times, excitement with the vision will be sufficient incentive. Alternatively, fear of what will happen if the organization fails to move toward the vision may serve as an incentive. Although important, neither fear nor rapture are necessarily sufficient.

If organizational members will lose their jobs or have their roles changed significantly, education that prepares them for new roles and or new jobs must be offered. Bonuses may be offered to key individuals, awarded according to the success of the change and each person's contribution to the change. At times, frankly, support is obtained through old-fashioned horse trading—if the other person will support the change, you will deliver something that is of interest to him or her (space, extra staff, a promotion). Incentives may also take the form of awards—for example, plaques and dinners for two—to staff who go above and beyond the call of duty during the change effort.

Planning, Implementing, Iterating. Change must be planned. These plans describe the tasks and task sequences necessary to effect the change. Tasks can range from redesigning forms to managing the staged implementation of application systems to retraining staff. Tasks must be allotted resources, and staff accountable for task performance must be designated.

Implementation of the plan is obviously necessary. Because few organizational changes of any magnitude will be fully understood beforehand, problems will be encountered during implementation. The new forms may fail to capture some necessary data. It may appear that the estimate of the time needed to register a patient is wrong and long lines are forming at the registration desk. It may turn out that the plan forgot to identify how certain information would flow from one department to another.

These problems are in addition to the problems that occur, for example, when task timetables slip and dependent tasks fall idle or are in trouble. The implementation of the application has been delayed and will not be ready when the staff move to the new building—what do we do? Iteration and adjustment will be necessary as the organization handles problems created when tasks encounter trouble and learns about glitches with the new processes and workflows.

Key Elements of Managing Projects

Within the overall change agenda, projects will be formed, managed, and completed. In large change initiatives, the IT project may be one of several projects. For several step-shift changes, the change management agenda may be composed almost entirely of the implementation of an application system.

Change management places an emphasis on many of the “softer,” although still critical, aspects of management and leadership: communicating vision, establishing trust, and developing incentives. Project management is a “harder” aspect of management. Project management centers on a set of management disciplines and practices that when executed well, increase the likelihood that a project will deliver the desired results. Project management has several objectives:

- Clearly define the scope and goals of the project.
- Identify accountability for the successful completion of the project and associated project tasks.
- Define the processes for making project-related decisions.
- Identify the project's tasks and task sequence and interdependencies.
- Determine the resource and time requirements of the project.
- Ensure appropriate communication with relevant stakeholders about project status and issues.

Different kinds of projects require different kinds of management strategies. Projects that are pilots or experiments require less formal oversight (and are not helped by large amounts of formal oversight) than large, multiyear, multimillion-dollar undertakings. Projects carried out by two or more organizations working together will have decision-making structures different from those found in projects done by several departments in one organization.

In this chapter we discuss a normative approach to managing relatively large projects within one organization. (Much of the following discussion is adapted from Spurr, 2003.) This approach is put in place once the need for the project has been established (through the IT strategy, for example), the project objectives have been defined, the budget has been approved, and the major stakeholders have been identified.

Project Roles

Four roles are important in the management of large projects:

- Business sponsor
- Business owner
- Project manager
- IT manager

Business Sponsor. The business sponsor is the individual who holds overall accountability for the project. The sponsor should represent the area of the organization that is the major recipient of the performance improvement that the project intends to deliver. For example, a project that involves implementing a new claims processing system may have the chief financial officer as the business sponsor. A project to improve nursing workflow may have asked the chief nursing officer to serve as business sponsor. A project that affects a very large portion of the organization may have the chief executive officer as the business sponsor.

The sponsor should be a member of a management or executive level that reflects the magnitude of the decisions and the support that the project will require. The more significant the undertaking, the higher the organizational level of the sponsor.

The business sponsor has several duties; he or she

- Secures funding and needed business resources—for example, the commitment of people's time to work on the project
- Has final decision-making and sign-off accountability for project scope, resources, and approaches to resolving project problems
- Identifies and supports the business owner(s) (discussed in the next section)
- Promotes the project internally and externally, and obtains the buy-in from business constituents
- Chairs the project steering committee and is responsible for steering committee participation during the life of the project
- Helps define deliverables, objectives, scope, and success criteria with identified business owners and the project manager
- Helps remove business obstacles to meeting the project timeline and producing deliverables, as appropriate

Business Owner. A business owner generally has day-to-day responsibility for running a function or a department—for example, a business owner might be the director of the clinical laboratories. A project may need the involvement of several business owners. For example, the success of a new patient accounting system may depend on processes that occur during registration and scheduling (and hence the director of outpatient clinics and the director of the admitting department will be business owners) and may also depend on adequate physician documentation of the care provided (and hence the administrator of the medical group will be a business owner).

Business owners often work on the project team. Among their several responsibilities they

- Represent their department or function at steering committee and project team meetings
- Secure and coordinate necessary business and departmental resources
- Remove business obstacles to meeting the project timeline and producing deliverables, as appropriate
- Work jointly with the project manager on several tasks (as described in the next section)

Project Manager. The project manager does just that—manages the project. He or she is the person who provides the day-to-day direction setting, conflict resolution, and communication needed by the project team. The project manager may be an IT staffer or a person in the business, or function, benefiting from the project. Among their several responsibilities, project managers

- Identify and obtain needed resources
- Deliver the project on time, on budget, and according to specification
- Communicate progress to sponsors, stakeholders, and team members
- Ensure that diligent risk monitoring is in place and appropriate risk mitigation plans have been developed
- Identify and manage the resolution of issues and problems
- Maintain the project plan
- Manage project scope

The project manager works closely with the business owners and business sponsor in performing these tasks. Together they set meeting agendas, manage the meetings, track project progress, communicate project status, escalate issues as appropriate, and resolve deviations and issues related to the project plan.

IT Manager. The IT manager is the senior IT person assigned to the project. He or she may be the boss of the project manager. In performing his or her responsibilities, the IT manager

- Represents the IT department
- Has final IT decision-making authority and sign-off accountability
- Helps remove IT obstacles to meeting project timelines and producing deliverables
- Promotes project internally and externally, and obtains buy-in from IT constituents

Project Committees

These four roles may employ two or three major committees to provide project guidance and management: a project steering committee, a project team, and a project review committee.

Project Steering Committee. The project steering committee provides overall guidance and management oversight of the project. The steering committee has the authority to resolve changes in scope that affect the budget, milestones, and deliverables. This committee is expected to resolve issues and address risks that cannot be handled by the project team. It also manages communications with the leadership of the organization and the project team. The project steering committee may be the same committee that leads the overall change process or a subcommittee of it.

The business sponsor should chair this committee. Its members should be representatives of the major areas of the organization that will be affected by the project and whose efforts are necessary if the project is to succeed. Returning to an earlier example, a steering committee overseeing the implementation of a new patient

accounting system might include the director of outpatient clinics, the director of the admitting department, and the medical group administrator as members. The senior IT manager should be on this committee. Depending on the size and importance of the project, this person could be the CIO. It is rare for the chair of the steering committee to be an IT person although having an IT person as a cochair is not uncommon.

Project Team. The project team may not be called a *committee*, but it will meet regularly and it does have responsibilities. The project manager chairs the project team. This team

- Manages the performance of the project work
- Resolves day-to-day project issues
- Manages and allocates resources as necessary to do the work
- Works with the steering committee and business owners, as necessary, to resolve problems; assess potential changes in scope, timeline, or budget; and communicate the status of the project

Project team members may be business owners, business owners' staff, IT managers, or IT managers' staff.

Project Review Committee. If the organization has a relatively large number of simultaneously active IT projects (say, fifty or so), a project review committee can be helpful. The project review committee focuses on a subset of all IT projects, those deemed to be the most important to the organization or the riskiest, or both. The review committee checks the status of each project in this subset to determine if the project is proceeding well or likely to be heading into trouble. If trouble is on the horizon, the committee discusses ways to reduce the threats to the project. The committee also looks for opportunities to leverage the work from one project across other projects and checks for areas where redundant work or work at cross-purposes may be occurring. For example, two projects may need large numbers of workstations deployed during the same interval of time. The IT group that deploys workstations cannot handle this volume. The project review committee would discuss ways to resolve this problem.

The review committee serves as a second pair of eyes on critical projects and has the ability to move resources between projects. For example, if Project A is experiencing instability with its core infrastructure, the review committee can pull network engineers and database server team members from Project B to help out on Project A. The review committee is often chaired by a senior IT person and is largely composed of IT project managers.

Project Management

Over the course of decades and millions of projects, a set of management disciplines and processes has been developed that helps to ensure that projects succeed. This collected set of practices is referred to as *project management*. One will see these disciplines and processes in action in any well-run project. Excellent project management does not ensure project success. However, without such project management the risks of failure skyrocket, particularly for large projects. The elements of project management (above and beyond the roles described earlier in this chapter) are reviewed in the following sections. These elements are created or established after the project proposal has been approved.

Project Charter

The project charter is a document that describes the purpose, scope, objectives, costs, and schedule for the project. This document also discusses the roles and responsibilities of the individuals and functions that must contribute to the project. The project charter serves three basic objectives:

- It ensures that planning assumptions or potentially ambiguous objectives are discussed and resolved (this occurs during development of the charter)
- It prevents participants from developing different understandings of the project intent, timeline, or cost
- It enables the project leadership to communicate as necessary with the organization about the project

The project charter sets out these project elements:

- Project overview and objectives
- Application features and capabilities (vision of the solution)
- Project scope and limitations
- Metrics for determining project success
- Budget and overall timetable
- Project organization
- Project management strategies

Appendix B contains an example of a project charter.

Project Plan

The project charter provides an overview of the project. The project plan provides the details of tasks, phases, and resources needed, by task and phase and timeline. The project plan is the tool used by the project team during the day-to-day management of the project. The project plan has several components:

- Project phases and tasks. A phase may have multiple tasks. For example, there may be a phase called “conduct analysis,” and it may involve such tasks as “review admitting department forms,” “document the admitting workflow,” and “document the discharge workflow.”
- The sequence of phases and tasks.
- Interdependencies between phases and tasks.
- The duration of phases and tasks.
- Staff resources needed, by task and phase.

Several software tools are available that assist project managers in developing project plans. These tools enable the project manager to develop the plan (as described earlier), prepare plan charts and resource use by task and phase, and model the impact on the plan if timelines change or resource availability alters.

Figure 14.1 is an example of a project timeline with project phases. Table 14.1 illustrates an analysis of project resources (staff) that shows project team members’ time commitment by activity.

Project Plan and Charter Considerations

Developing project plans and charters requires skill and experience. Managers are often in forums (such as project steering committee meetings) where they are asked to review, critique, and approve a project plan. What should they look for in these plans?

To a large degree, the reputations of project managers precede them. If project managers have proven themselves over the course of many projects, then their plans are likely to be generally sound. If project managers are novices or have an uneven track record, their plans may require greater scrutiny. Regardless of track record, there are several cues that a project plan is as solid as one can make it at the inception of the project:

- The plan charter is clear and explicit. Fuzzy objectives and vague understandings of resource needs indicate that the plan needs further discussion and development.
- The leaders of the departments and functions that will be affected by the plan or that need to devote resources to the plan have reviewed the charter and plan, their concerns have been heard and addressed, and they have publicly committed to performing the work needed in the plan.

FIGURE 14.1. PROJECT TIMELINE WITH PROJECT PHASES.

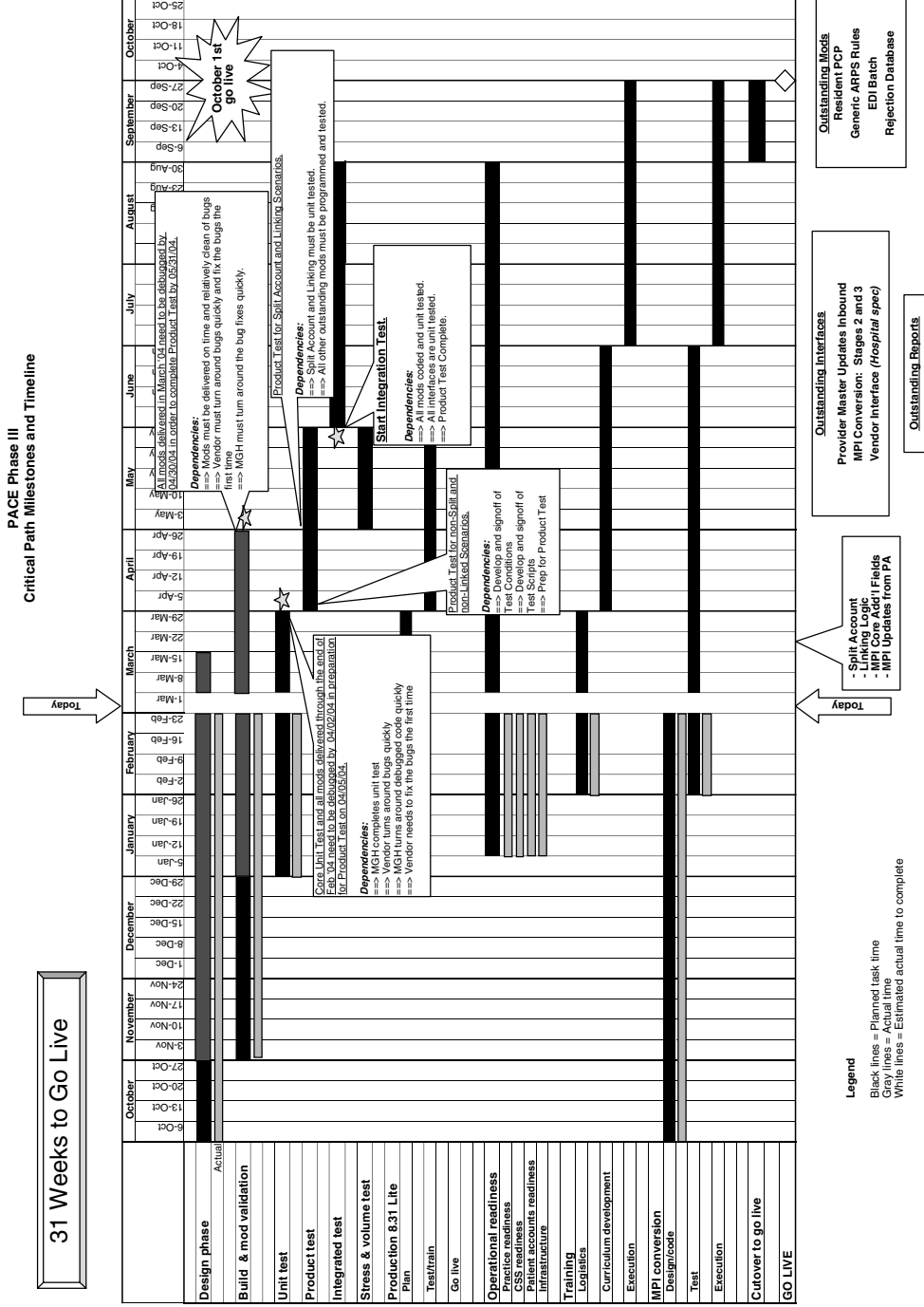


TABLE 14.1. PROJECT RESOURCE ANALYSIS.

Project	Activity	Start Activity	Finish Activity	% Allocated*
Susan Smith				
DFCI - CRIS --> Cancer Registry Data Load	Application Design	11/3/03	11/10/03	18.95%
DFCI - CRIS --> Cancer Registry Data Load	Application Testing	11/3/03	12/12/03	25.38%
DFCI - CRIS --> Cancer Registry Data Load	Data mapping specification	11/3/03	11/19/03	17.25%
DFCI - CRIS --> Cancer Registry Data Load	Functional Analysis	11/3/03	11/14/03	35.00%
DFCI - CRIS Minor Enhancements	CRIS breast minor enhancements analysis	11/3/03	11/2/04	4.75%
DFCI - CRIS Minor Enhancements	CRIS breast minor enhancements testing	11/3/03	11/2/04	4.75%
DFCI CRIS/STIP GI Development and Implementation	GI CRA form design/analysis	11/3/03	1/29/04	5.38%
DFCI CRIS/STIP GI Development and Implementation	GI follow-up form design/analysis	11/3/03	2/6/04	5.75%
DFCI Renal STIP/CRIS	Renal CRIS analysis	11/3/03	2/5/04	
	Administration	11/3/03	9/30/04	12.63%
	Support work	11/3/03	9/30/04	55.50%
James Jones				
BICS Modernization	Background research	11/3/03	10/28/04	19.50%
BICS Modernization	Develop overall project plan	11/3/03	12/13/04	8.50%
BICS Modernization	E-Mail coding	11/3/03	1/15/04	10.00%
Garner TCO Analysis	Collect data and input into template — Rd 1	11/3/03	11/11/03	8.55%
LDRPS Implementation	Plan building pilot group	11/3/03	12/1/03	11.00%
PHS Document Management	VDRNETS security testing	11/3/03	11/11/03	
	Administration	11/3/03	9/30/04	19.50%
	Support work	11/3/03	9/30/04	24.40%

* Percentage of employee's time devoted to a project during the interval bounded by the "start activity" date and the "finish activity" date.

- The project timelines have been reviewed by multiple parties for reasonableness, and these timelines have taken into consideration factors that will affect the plan—for example, key staff going on vacation or organizational energies being diverted to develop the annual budget—and any uncertainties that might exist for particular phases or tasks—for example, if it is not fully clear how a specific task will be performed, that task timeline should have some “slack” built into it.
- The resources needed have been committed. The budget has been approved. Staff needed by the plan can be named, and their managers have taken steps to free up the staff time needed by the plan.
- The accountabilities for the plan and for each plan phase and task are explicit.
- Project risks have been comprehensively assessed, and thoughtful approaches to addressing each risk developed. Some examples of project risks are unproven information technology, a deterioration in the organization's financial condition, and turnover of project staff.
- A reasonable amount of contingency planning has addressed inevitable problems and current uncertainties. In general, projects should add 10 percent to the timeline and 10 percent to the budget to reflect the time and dollar cost of inevitable problems. For very complex projects, it is not unusual to see 20 to 25 percent of the budget and the duration of some tasks labeled “unknown” or “unclear.”

Project Status Report

The project status report documents and communicates the status of the project. This report is generally prepared monthly and distributed to project participants and stakeholders. The status report often provides matter for discussion at steering committee meetings. It typically covers recent accomplishments and decisions, work in progress, upcoming milestones, and issues that require resolution (see the example in Figure 14.2). It may use a green (task or phase proceeding well), yellow (task or phase may be facing a timeline or other problem), and red (task or phase is in trouble and requires attention) color scheme when graphically depicting the status of a project. When a plethora of tasks and phases are tagged with red, then the project is experiencing significant difficulty. Conversely, a sea of green indicates that the project is going well.

The preparation, distribution, and discussion of the project status report are part of the overall project communication plan. Other important communications might include quarterly project presentations at meetings of the organization's department heads, articles about the project in the organization's internal newsletter, and presentations at

FIGURE 14.2. PROJECT STATUS REPORT.

Electronic Medication Administration Record (e-MAR) - Status Report
Reporting Period: July 2003

Business Sponsor: Sally Martin, RN, Vice President Patient Care Services

Business Owners: Amy Lawson RN, Director of Nursing Quality and Practice; William Smith RPh, Director of Pharmacy

Information Systems Sponsors: Cindy Martin RNC, Corporate Director of Clinical Systems Management; Sue Moore CIO-BWH

PROJECT SCHEDULE

Activity	Planned	Revised	Actual Delivery
Functional specification requirements completed	01/03	07/03	07/03
Technical specifications completed	02/03	11/28/03	
Wireless infrastructure in place for pilot pods	02/03	9/15/03	
Wireless infrastructure in place for training room (Ledge Site)	02/03	07/03	07/03
Wireless infrastructure in place for pharmacy	02/03	05/03	06/03
Wireless infrastructure in place for all adult inpatient pods	03/03	09/26/03	
Bar code development – medications	06/03	08/29/03	
Bar code development – patient ID band implementation	05/03	08/15/03	
Bar code development – clinical staff implementation (employee ID)	05/03	08/15/03	
Bar code imager selection	02/03	04/03	04/03
Adult pharmacy development	06/03	08/03	
Adult pharmacy application pilot	08/05	08/25	
Code freeze (pilot)	04/03	09/15/03	
Integrated testing (pilot)	04/03	9/15/03 – 10/25/03	
Pilot			
Hardware purchase (notebook, imager)	06/03	07/03	07/03
Create image/test Fujitsu Lifebook	06/03	07/03	07/03
Hiring/training support staff	07/03	09/26/03	
Hardware deployment	08/03	10/27/03	
Training – planning complete	06/03	07/03	07/03
Training – development complete	07/03	10/01/03	
Training – conduct classes	08/03	10/14 – 10/25	
Implementation	06/03	10/27	
Evaluation of pilot	07/03	12/03	
Rollout			
Rollout implementation plan	09/03	08/29/03	
Hiring support staff	12/03	01/ 04	
Training support staff	01/04	01/ 04	
Hardware deployment	07/03	2/04 – 5/04	
Training – planning	08/03	12/04	
Training – development	09/03	01/ 04	
Training – conduct classes	09/03	02/01/04 – 05/03/04	
Implementation begins	10/03	02/16/04	
Implementation ends	04/04	05/21/04	

Accomplishments

- The functional requirements for the pilot have been agreed upon and finalized.

Decisions

- The pilot date was revised to 10/27 – 11/21. The additional time is needed to complete the application development for upcoming changes to OE, such as the new KCL scales and PCA templates.
- The format for the Medical Record Copy of the e-MAR was approved by Health Information Systems.

Work in Progress

- Completing the bar-coded employee ID badge. This should be ready for testing during the second week in August.
- Completing the bar-coded patient ID band, which can be finalized when the font software arrives.
- Programming for recently finalized e-MAR specifications — scales, tapers, various templates, downtime procedures, reports, etc.
- Programming for BICS changes necessary for e-MAR.
- Anne Williams is working with several cart vendors to secure carts for the pilot.
- Wiring/cabling for the wireless network on the inpatient pods begins 8/4 and continues through 9/26.
- Planning for integration testing.
- Unit testing.

Issues

- Accessing BICS from the Web pod monitor is inconsistent and slow. The platform architecture specialists are investigating a solution, and it is being tested now.
- The font software for patient ID bands has been delayed. Joanne Jones is working to expedite this so that final development can occur.

Upcoming Activities

- ID badge replacement scheduled for RNs and pharmacists 8/14 – 8/22.
 - The pharmacy will conduct a pilot of its new Web system beginning on 8/25.
-

specific leadership forums—for example, at a medical staff forum or at a meeting of the board or of the executive committee.

Factors That Contribute to IT Initiative Failures

The rate of failure of IT initiatives is surprisingly high. Project failure occurs when a project is significantly over budget, takes much longer than the estimated timeline, or has to be terminated because so many problems have occurred that proceeding is no longer judged to be viable. Severance and Passino (2002) estimate that one-third of all IT projects are cancelled before completion, and only 10 percent achieve their original plan. Among the remainder, budget and schedule overruns approach 100 percent, and the functionality delivered is less than half of what was originally anticipated.

Cash, McFarlan, and McKenney (1992) note that two major categories of risk confront significant IT investments: strategy failures and implementation failures. The project failure rates suggest that management should be more worried about IT implementation than IT strategy. IT strategy is sexier and more visionary than implementation. However, a very large number of strategies and visions go nowhere or are diminished because the organization is unable to implement them.

Why is this failure rate so high? What happens?

In the sections that follow, we will examine several classes of barriers that hinder large IT projects.

Lack of Clarity of Purpose

Any project or initiative is destined for trouble if its objectives and purpose are unclear. Sometimes the purpose of a project is only partially clear. For example, the organization may have decided that it should implement an electronic medical record (EMR) in an effort to “improve the quality and efficiency of care.” However, it is not really clear to the leadership and staff how the EMR will be used to improve care. Will problems associated with finding a patient’s record be solved? Will the record be used to gather data about care quality? Will the record be used to support outpatient medication ordering and reduce medication error rates?

All these questions can be answered yes, but the organization never got beyond the slogan of “improve the quality and efficiency of care.” As a result the scope of the project is murky. The definition of care improvement is left up to the project participant to interpret. And the scope and timetable of the project cannot possibly be precise because project objectives are too fuzzy.

Lack of Belief in the Project

At times the objectives are very clear, but the members of the organization are not convinced that the project is worth doing at all. Because the project will change the work life of many members and require that they participate in design and implementation, they need to be sufficiently convinced that the project will improve their lives or is necessary if the organization is to thrive. They will legitimately ask, What’s in it for me? Unconvinced of the need for the project, they will resist it. A resistant organization will doom any project. Projects that are viewed as illegitimate by a large portion of the people in an organization rarely succeed.

Insufficient Leadership Support

The leadership may be committed to the undertaking yet not demonstrate that commitment. For example, leaders may not devote sufficient time to the project or may decide to send subordinates to meetings. This broadcasts a signal to the organization

that the leaders have other, “more important” things to do. Tough project decisions may get made in a way that shows the leaders are not as serious as their rhetoric, because when push came to shove, they caved in.

Members of the leadership team may have voted yes to proceed with a project, but their votes may not have included their reservations about the utility of the project or the way it was put together. Once problems are encountered in the project (and all projects encounter problems), this qualified leadership support evaporates, and the silent reservations become public statements such as, “I knew that this would never work.”

Organizational Inertia

Even when the organization is willing to engage in a project, inertia can hinder it. People are busy. They are stressed. They have jobs to do. Some of the changes are threatening. Staff may believe these changes leave them less skilled or less instrumental or with reduced power. Or they may not have a good understanding of work life after the change, and they may imagine that an uncertain outcome cannot be a good outcome.

Projects add work on top of the workload of already overburdened people. Projects add stress for already stressed people. As a result, despite the valiant efforts of leadership and the expenditure of significant resources, a project may slowly grind to a halt because too many members find ways to avoid or not deal with the efforts and changes the initiative requires. Bringing significant change to a large portion of the organization is very hard because, if nothing else, there is so much inertia to overcome.

Organizational Baggage

Organizations have baggage. Baggage comes in many forms. Some organizations have no history of competence in making significant organizational change. They have never learned how to mobilize the organization's members. They do not know how to handle conflict. They are unsure how to assemble and leverage multidisciplinary teams. They have never mastered staying the course, over years, during the execution of complex agendas. These organizations are “incompetent,” and this incompetence extends well beyond IT, although it clearly includes IT initiatives.

An organization may have tried initiatives like “this” before and failed. The proponents of the initiative may have failed at other initiatives. Organizations have very long memories and their members may be thinking something like, “The same clowns who brought us that last fiasco are back with an even better idea.” The odor from prior failures significantly taints the credibility of newly proposed initiatives and helps to ensure that organizational acceptance will be weak.

Lack of an Appropriate Reward System

Aspects of organizational policies, incentives, and practices can hinder a project. The organization's incentive system may not be structured to reward multidisciplinary behavior—for example, physicians may be rewarded for research prowess or clinical excellence but not for sitting on committees to design new clinical processes. An integrated delivery system may have encouraged its member hospitals to be self-sufficient. As a result, management practices that involve working across hospitals never matured, and the organization doesn't know how (even if it is willing) to work across hospitals.

Lack of Candor

Organizations can create environments that do not encourage healthy debate. Such environments can result when leadership is intolerant of being challenged or has an inflated sense of its worth and does not believe that it needs team effort to get things done. The lack of a climate that encourages conflict and can manage conflict means that initiative problems will not get resolved. Moreover, organizational members, not having had their voices heard, will “tolerate” the initiative only out of the hope that they will outlast the initiative and the leadership.

Sometimes the project team is uncomfortable delivering bad news. Project teams will screw up and make mistakes. Sometimes they really screw up and make really big mistakes. Because they may be embarrassed, or worried that they will get beaten up, they hide the mistakes from the leadership and attempt to fix the problems without “anyone having to know.” This attempt to hide bad news is a recipe for disaster. It is unrealistic to expect problems to go unnoticed; invariably the leadership team finds out about the problem and its trust in the project team erodes. At times, leadership has to look in the mirror to see if its own intolerance for bad news in effect created the problem.

Project Complexity

Project complexity is determined by many factors:

- The number of people whose work will be changed by the project and the depth of those changes
- The number of organizational processes that will be changed and the depth of those changes
- The number of processes between the organization and other organizations that will be changed and the depth of those changes
- The interval over which all this change will occur—for example, will it occur quickly or gradually?

If the change is significant in scale, scope, and depth then it becomes very difficult (often impossible) for the people managing the project to truly understand what the project needs to do. The design will be imperfect. The process changes will not integrate well. And many curves will be thrown the project's way as the implementation unfolds and people realize their mistakes and understand what they failed to understand initially.

Sometimes complex projects disappear in an organizational mushroom cloud. The complexity overwhelms the organization and causes the project to crash suddenly. More common is the "death by ants"—no single bite (or project problem) will kill the project, but a thousand will. The organization is overwhelmed by thousands of small problems and inefficiencies and terminates the undertaking.

One should remember that complexity is relative. Organizations generally have developed a competency to manage projects up to a certain level and type of complexity. Projects that require competency beyond that level are inherently risky. A project that is risky for one organization may not be risky for another. For example, an organization that typically manages projects that cost \$2 million, take ten person-years of effort, and affect 300 people will struggle with a project that costs \$20 million and is a one-hundred-person-year effort (Cash, McFarlan, and McKenney, 1992).

Failure to Respect Uncertainty

Significant organizational change brings a great deal of uncertainty with it. The leadership may be correct in its understanding of where the organization needs to go and the scope of the changes needed. However, it is highly unlikely that anyone really understands the full impact of the change and how new processes, tasks, and roles will really work. At best, leadership has a good approximation of the new organization. The belief that a particular outcome is certain can be a problem in itself.

Agility and the ability to detect when a change is not working and to alter its direction are very important. Detection requires that the organization listens to the feedback of those who are waist deep in the change and is able to discern the difference between organizational noise that comes with any change and organizational noise that reflects real problems. Altering direction requires that the leadership not cling to ideas that cannot work and also be willing to admit to the organization that it was wrong about some aspects of the change.

Undernourished Initiatives

There may be a temptation, particularly as the leadership tries to accomplish as much as it can with a constrained budget, to tell a project team, "I know you asked for ten people, but we're going to push you to do it with five." The leadership may believe that

such bravado will make the team work extra hard and, through heroic efforts, complete the project in a grand fashion. However, bravado may turn out to be bellicose stupidity. This approach may doom a project, despite the valiant efforts of the team to do the impossible.

Another form of undernourishment involves placing staff other than the best staff on the initiative. If the initiative is very important, then it merits using the best staff possible and freeing up their time so they can focus on the initiative. An organization's best staff are always in demand, and there can be a temptation to say that it would be too difficult to pull them away from other pressing issues. They are needed elsewhere and this decision is difficult. However, if the initiative is critical to the organization, then those other demands are less important and can be given to someone else. Critical organizational initiatives should not be staffed with the junior varsity.

Failure to Anticipate Short-Term Disruptions

Any major change will lead to short-term problems and disruptions in operations. Even though current processes can be made better, they did work and staff knew how to make them work. When processes are changed, there is a shakeout period as staff adjust and learn how to make the new processes work well. At times, adjusting to the new application system is the core of the disruption. This shakeout period can go on for months. Shakeout periods bring degradation in organizational performance. Service will deteriorate. Days in accounts receivable will climb. Balls will be dropped in many areas. The organization can misinterpret these problems as a sign that the initiative is failing.

Listening closely to the issues and suggestions of the front line is essential during this time. These staff need to know that their problems are being heard and that their ideas for fixing these problems are being acted upon. People often know exactly what needs to be done to remove system disruptions. Listening to and acting on their advice also improves their buy-in to the change.

While working hard to minimize the duration and depth of disruption, the organization needs to be tolerant during this period and to appreciate the low-grade form of hell that the staff is enduring. It is critical that this period be kept as short and as pain free as possible. If the disruption lasts too long, staff may conclude that the change is not working and abandon their support.

Invisible Progress

Sometimes initiatives are launched with great fanfare. Speeches are made outlining the rationale for the initiative. Teams are formed. Budgets are established. The organization is ready to move. Then nothing seems to be happening.

Large, complex initiatives often involve large amounts of preparatory analysis and work. These initiatives may also involve implementing a significant IT foundation of

new networks and databases. And while the project teams are busy, the rest of the organization sees no progress and comes to believe that the initiative is being held hostage. Action-oriented managers want to know what happened to the action.

Change initiatives and IT projects need to regularly communicate their progress even if that progress is largely unseen by the organization. In a similar fashion the progress made in digging a new tunnel might be invisible to the motorist until the tunnel is open, but the tunnel diggers can regularly report on the work that is being done underground.

If possible, the project should seek to produce a series of short-term deliverables, even if they are small. For example, while the IT team is performing foundational work, the organization might go ahead and make some process changes without waiting for the implementation of the application. Deliverables demonstrate that progress is being made and help to sustain organizational commitment to the initiative. Organizational commitment is like a slowly leaking balloon; it must be constantly reinflated.

Lack of Technology Stability and Maturity

Information technology may be obviously immature. New technologies are being introduced all the time, and it takes time for a technology to work through its “kinks” and achieve an acceptable level of stability, supportability, and maturity. Wireless networks and devices are current examples of information technologies that are in their youth.

Organizations can become involved in projects that require immature technology to play a critical role. This clearly elevates the risk of the project. The technology will suffer from performance problems, and the organization's IT staff and the technology supplier may have limited ability to identify and resolve technology problems. Organizational members, tired of the instability, become tired of the project and it fails.

In general it is not common, nor should it be often necessary, for a project to hinge on the adequate performance of new technology. A thoughtful assessment that a new technology has potentially extraordinary promise and that the organization can achieve differential value by being an early adopter should precede any such decision. Even in these cases, pilot projects that provide experience with the new technology while limiting the scope of its implementation (which minimizes potential damage) are highly recommended.

The organization should remember that technology maturity is also relative. Even if the rest of the world has used a technology, if it is new to your vendor and new to your IT staff, then it should be considered immature. Your vendor and staff will need to learn, often the hard way, how to manage and support this technology.

Projects can also get into trouble when the amount of technology change is extensive. For example, the organization may be attempting to implement, over a short

period of time, applications from several different vendors that involve different operating systems, network requirements, security models, and database management systems. This broad scope can overwhelm the IT department's ability to respond to technology misbehavior.

How You Can Avoid These Mistakes

Major IT projects fail in many ways. However, a large number of these failures involve management action or inaction. Few management teams and senior leaders start IT projects hoping that failure is the outcome. Summarizing our discussion in this chapter produces a set of recommendations that can help organizations reduce the risk of failure:

- Ensure that the objectives of the IT initiative are clear.
- Communicate the objectives and the initiative, and test the degree to which organizational members have bought into them.
- Publicly demonstrate your conviction by “being there” and showing resolve during tough decisions.
- Respect organizational inertia, and keep hammering away at it.
- Distance the project from any organizational baggage, perhaps through your choice of project sponsors and managers.
- Change the reward system if necessary to create incentives for participants to work toward project success.
- Accept and welcome the debate that surrounds projects, invite bad news, and do not hang those who make mistakes.
- Address complexity by breaking the project into manageable pieces, and test for evidence that the project might be at risk by trying to do too much all at once.
- Realize that there is much that you do not know about how to change the organization or the form of new processes; be prepared to change direction and listen and respond to those who are on the front line.
- Supply resources for the project appropriately, and assign the project to your best team.
- Try to limit the duration and depth of the short-term operational disruption, but accept that it will occur.
- Ensure and communicate regular, visible progress.
- Be wary of new technology and projects that involve a broad scope of information technology change.

These steps, along with solid project management, can dramatically reduce the risk that an IT project will fail. However, these steps are not foolproof. Major IT

projects, particularly those accompanied by major organizational change, will always have a nontrivial level of risk.

There will also be times when a review of the failure factors indicates that a project is too risky. The organization may not be ready; there may be too much baggage, too much inertia to overcome; the best team may not be available; the organization may not be good at handling conflict; or the project may require too much new information technology. Projects with considerable risk should not be undertaken until progress has been made in addressing the failure factors. Management of IT project risk is a critical contributor to IT success.

Perspective: Critical Success Factors

Jay Toole outlines several critical success factors for successful clinical information system (CIS) implementation and transformation of clinical processes.

- Set realistic and clear expectations for the outcomes that will result from implementing the CIS.
- Recognize that implementing a CIS and transforming care processes is an operational initiative and not an IT initiative.
- Operational executives must take ownership of the implementation and related transformation and must be held accountable for its success.
- Clinicians must actively participate in the CIS design and implementation.
- A liaison person knowledgeable in both IT and medical issues should be designated to keep the physicians engaged in the implementation process.
- A strong project manager with CIS implementation experience needs to be dedicated to the initiative. [He or she] must have dedicated staff resources with the right mix of clinical, operational and technical expertise.
- A well-defined implementation plan and the ability to monitor and track results against the plan is crucial.
- Incentives must be aligned and these incentives should reward all participants for successful implementation and achievement of predefined outcomes.

Toole, 2003

Perspective: IT Project Implementation Checklist

Andrew McAfee has developed a short checklist for managers who are overseeing the implementation of IT projects. This checklist covers critical project management actions necessary to avoid disaster:

- *Treat the implementation as a business change effort* and not as a technology installation. Project leadership should come from the business side, and the business

sponsor should be given the authority to make project decisions and be held accountable for project outcomes.

- *Devote the necessary resources to the project.* This means putting your best people on the project and avoiding cutting corners on budgets and the use of outside expertise.
- *Make sure that goals, scope, and expectations are clear from the outset.* Projects get in trouble when they are overhyped, scope is allowed to expand without discipline, and goals are fuzzy.
- *Track the project's progress, results, and scope.* Sound project management—for example, status reports, milestones, methodical reviews of proposals to change scope, and budget tracking—must be in place.
- *Test the new system every way that you can before you go live.* Testing and retesting helps minimize unpleasant surprises, technology problems, and poor fit with workflow.
- *Secure top management commitment.* The leadership must believe in the project—its goals, scope, and the project team. Leadership must also soberly understand the magnitude and difficulty of the undertaking.

Adapted from McAfee, 2003

Summary

The leadership of health care organizations plays an essential role in managing the change that invariably accompanies the implementation of an IT application. This role is particularly important in step-shift, radical, and transformational change. The leadership must lead, establish a vision, communicate, manage trust, plan the change, implement the change, and iterate as the organization experiences the change.

The hard science of implementation requires the creation of roles such as the business sponsor and project managers and committees such as the project steering committee and project teams. Solid project management techniques must be in place—for example, project charters and project plans must be created and project communication must be carried out.

There are many ways that a project failure can occur; unclear objectives, embryonic information technology, or failure to anticipate short-term operational disruptions may lead to failure, for example. It is the responsibility of the organization's leadership to minimize the occurrence and severity of the factors that threaten to undermine the change.

Chapter Fourteen: Learning Activities

1. Attend a project team meeting for each of two different projects. Describe the project and the challenges facing the project teams. Comment on the differences between the teams and the projects.
2. Interview the business sponsor of a major project. Describe the role of this business sponsor. Discuss the scope of the project and its objectives. Describe the change strategy for the project.
3. Interview a project manager. Describe the factors and skills that they associate with successful projects.



CHAPTER FIFTEEN

ASSESSING AND ACHIEVING VALUE IN HEALTH CARE INFORMATION SYSTEMS

Virtually all the discussion in this book has focused on the knowledge and management processes necessary to achieve one fundamental objective: organizational investments in IT resulting in a desired value. That value might be the furtherance of organization strategies, improvement in the performance of core processes, or the enhancement of decision making. Achieving value requires the alignment of IT with overall strategies, thoughtful governance, solid information system selection and implementation approaches, and effective organizational change.

Failure to achieve desired value can result in significant problems for the organization. Money is wasted. Execution of strategies is hamstrung. Organization processes can be damaged.

This chapter carries the IT value discussion further. Specifically, it covers the following topics:

- The nature of IT-enabled value
- The IT project proposal
- Steps to improve value realization
- Why IT investment fails to deliver returns
- Analyses of the IT value challenge

The Nature of IT-Enabled Value

We can make several observations about the nature of IT-enabled value:

- IT value can be both tangible and intangible.
- IT value can be significant.
- IT value can be diverse across IT proposals.
- A single IT investment can have a diverse value proposition.
- Different IT investments have different objectives and hence different value propositions and value assessment techniques.

These observations will be discussed in more detail in the following sections.

IT Value Can Be Both Tangible and Intangible

Tangible value can be measured whereas intangible value is very difficult, perhaps practically impossible, to measure.

Some tangible measures can be expressed in terms of dollars:

- Increases in revenue
- Reductions in labor costs—for example, through staff layoffs, overtime reductions, or shifting work to less expensive staff
- Reductions in supplies needed—for example, paper
- Reductions in maintenance costs for computer systems
- Reductions in use of patient care services—for example, fewer lab tests are performed or care is conducted in less expensive settings

Some tangible measures can be expressed in terms of process improvements:

- Fewer errors
- Faster turnaround times for test results
- Reductions in elapsed time to get an appointment
- A quicker admissions process
- Improvement in access to data

Some tangible measures can be expressed in terms of strategically important measures:

- Growth in market share
- Reduction in turnover

- Increase in brand awareness
- Increase in patient and provider satisfaction
- Improvement in reliability of computer systems

In contrast, intangible value can be very difficult to measure. One is trying to measure such things as

- Improvements in decision making
- Improvements in communication
- Improvements in compliance
- Improvements in collaboration
- Increases in agility
- Becoming more state of the art
- Improvements in organizational competencies—for example, the organization is better at managing chronic disease
- Becoming more customer friendly

IT Value Can Be Significant

Glaser, DeBor, and Stuntz (2003) describe the return achieved by replacing the manual approach to determining patient eligibility for coverage with an electronic data interchange (EDI) based approach. One hospital estimated that for an initial investment of \$250,000 in eligibility interface development and rollout effort, plus an annual maintenance fee of \$72,000, it could achieve ongoing annual savings of approximately \$485,000. This EDI investment return was achieved within a year of operation.

Wang et al. (2003) performed an analysis of the costs and benefits of the electronic medical record (EMR) in primary care. This sophisticated analysis explored the return over a range of EMR capabilities (from basic to advanced), practice sizes (small to large), and reimbursement structures (from entirely fee-for-service to extensive risk-sharing arrangements). On average the net estimated benefit was \$86,000 per provider over five years.

Bates et al. (1998) found that a 55 percent reduction in serious medication errors resulted from implementing inpatient provider order entry at the Brigham and Women's Hospital. The computerized order entry system highlighted, at the time of ordering, possible drug allergies, drug-drug interactions, and drug-lab result problems.

IT Value Can Be Diverse Across IT Proposals

Consider three proposals (real ones from a large integrated delivery system) that might be in front of organizational leadership for review and approval: a disaster notification system, a document imaging system, and an e-procurement system. Each has a different type of value to the organization.

The *disaster notification system* would enable the organization to page critical personnel, inform them that a disaster—for example, a train wreck or biotoxin outbreak—had taken place, and tell them the extent of the disaster and the steps they need to take to help the organization respond to the disaster. The system would cost \$520,000. The value would be “better preparedness for a disaster.”

The *document imaging system* would be used to electronically store and retrieve scanned images of paper documents, such as payment reconciliations, received from insurance companies. The system would cost \$2.8 million, but would save the organization \$1.8 million per year (\$9 million over the life of the system) due to reductions in the labor required to look for paper documents and in the insurance claim write-offs that occur because a document cannot be located.

The *e-procurement system* would enable users to order supplies, ensure that the ordering person had the authority to purchase supplies, transmit the order to the supplier, and track the receipt of the supplies. Data from this system could be used to support the standardization of supplies: that is, to reduce the number of different supplies used. Such standardization might save \$500,000 to \$3 million per year. The range of savings would depend on physician willingness to standardize. The system would cost \$2.5 million.

These proposals reflect a diversity of value, ranging from “better disaster response” to a clear financial return (document imaging) to a return with such a wide range (e-procurement) that it could be a great investment (if you really could save \$3 million a year) or a terrible investment (if you could save only \$500,000 a year).

A Single IT Investment Can Have a Diverse Value Proposition

Picture archival and communication systems (PACS) are used to store radiology (and other) images, support interpretation of an image, and distribute the information to the physician providing direct patient care. A PACS can

- Reduce costs for radiology film and the need for film librarians
- Improve service to the physician delivering care, through improved access to images
- Improve productivity for the radiologists and for the physicians delivering care (both groups reduce the time they spend looking for images)
- Generate revenue, if the organization uses the PACS to offer radiology services to physician groups in the community

This one investment has the potential to deliver cost reduction, productivity gains, service improvements, and revenue gains.

Different IT Investments Have Different Objectives and Hence Different Value Propositions and Value Assessment Techniques

The Committee to Study the Impact of Information Technology on the Performance of Service Activities (1994), organized by the National Research Council, has identified six categories of IT investments reflecting different objectives. The techniques used to assess IT investments should vary by the type of objective that the IT investment intends to support. One technique does not fit all IT investments.

Perspective: Four Types of IT Investment

Jeanne Ross and Cynthia Beath studied the IT investment approaches of thirty companies from a wide range of industries. They identified four different classes of investment:

- *Transformation.* These IT investments had an impact that would affect the entire organization or a large number of business units. The intent of the investment was to effect a significant improvement in overall performance or change the nature of the organization.
- *Renewal.* Renewal investments were intended to upgrade core IT infrastructure and applications or reduce the costs or improve the quality of IT services. Examples of these investments include application replacements, upgrades of the network, or expansion of data storage.
- *Process improvement.* These IT investments sought to improve the operations of a specific business entity—for example, to reduce costs and improve service.
- *Experiments.* Experiments were designed to evaluate new information technologies and test new types of applications. Given the results of the experiments, the organization would decide whether broad adoption was desirable.

Different organizations will allocate their IT budgets differently across these classes. An office products company had an investment mix of experiments (15 percent), process improvement (40 percent), renewal (25 percent), and transformation (20 percent). An insurance firm had an investment mix of experiments (3 percent), process improvement (25 percent), renewal (18 percent), and transformation (53 percent).

The investment allocation is often an after-the-fact consideration—the allocation is not planned, it just “happens.” However, ideally, the organization decides its desired allocation structure and does so before the budget discussions. An organization with an ambitious and perhaps radical strategy may allocate a very large portion of its IT investment to the transformation class whereas an organization with a conservative, stay-the-course strategy may have a large process improvement portion to its IT investments.

Ross and Beath, 2002

Infrastructure. IT investments may be for infrastructure that enables other investments or applications to be implemented and deliver desired capabilities. Examples of infrastructure include data communication networks, workstations, and clinical data repositories. A delivery system-wide network enables the organization to implement applications to consolidate clinical laboratories, implement organization-wide collaboration tools, and share patient health data between providers.

It is difficult to quantitatively assess the impact or value of infrastructure investments because

- They enable applications. Without those applications, infrastructure has no value. Hence infrastructure value is indirect and depends on application value.
- The allocation of infrastructure value across applications is complex. When millions of dollars are invested in a data communication network, it may be difficult or impossible to determine how much of that investment should be allocated to the ability to create delivery system-wide EMRs.
- A good IT infrastructure is often determined by its agility, its potency, and its ability to facilitate integration of applications. It is very difficult to assign return on investment numbers or any meaningful numerical value to most of these characteristics. What, for instance, is the value of being agile enough to speed up the time it takes to develop and enhance applications?

Information system infrastructure is as hard to evaluate as other organizational infrastructure, such as having talented, educated staff. As with other infrastructure:

- Evaluation is often instinctive and experientially based.
- In general, underinvesting can severely limit the organization.
- Investment decisions involve choosing between alternatives that are assessed based on their ability to achieve agreed-upon goals. For example, if we wish to improve security, we might ask whether we should invest in network monitoring tools or enhanced virus protection. Which of these investments would enable us to make the most progress toward our goal? Our goals too may be difficult to quantify in terms of dollars. For example, our goals might be to move images across the system, to greatly increase information system availability, to have improved security, to have rapid application development.

Mandated. Information system investment may be necessary because of mandated initiatives. Mandated initiatives might involve reporting quality data to accrediting organizations, making required changes in billing formats, or improving disaster notification systems. Assessing these initiatives is generally approached by identifying the

least expensive and the quickest to implement alternative that will achieve the needed level of compliance.

Cost Reduction. Information system investments directed to cost reduction are generally highly amenable to return on investment (ROI) and other quantifiable dollar-impact analyses. The ability to conduct a quantifiable ROI analysis is rarely the question. The ability of management to effect the predicted cost reduction or avoidance is often a far more germane question.

Specific New Products and Services. IT can be critical to the development of new products and services. At times the information system delivers the new service, and at other times it is itself the product. Examples of information system-based new services include bank cash management programs and programs that award airline mileage for credit card purchases. A new service offered by some health care providers is an Internet portal that enables patients to communicate with their physician and access care guidelines and consumer-oriented medical textbooks. The value of some of these new products and services can be quantifiably assessed in terms of a monetary return. These assessments include analyses of potential new revenue, either directly from the service or from service-induced use of other products and services. A return-on-investment analysis will need to be supplemented by techniques such as sensitivity analyses of consumer response. Despite these analyses the value of the IT investment usually has a speculative component. This component involves consumer utilization, competitor response, and impact on related businesses.

Quality Improvement. Information system investments are often directed to improving the quality of service or medical care. These investments may be intended to reduce waiting times, improve the ability of physicians to locate information, improve treatment outcomes, or reduce errors in treatment. Evaluation of these initiatives, although quantifiable, is generally done in terms of service parameters that are known or believed to be important determinants of organizational success. These parameters might be measures of aspects of organization processes that customers encounter and then use to judge the organization—for example, waiting times in the physician's office. A quantifiable dollar outcome of service of care quality improvement can be very difficult to predict. Service quality is often necessary to protect current business and the effect of a failure to continuously improve service or medical care can be difficult to project.

Major Strategic Initiative. Strategic initiatives in information technology are intended to significantly change the competitive position of the organization or redefine the core nature of the enterprise. In health care it is rare that information systems

are the centerpiece of a redefinition of the organization. However, other industries have attempted IT-centric transformations. Amazon.com is an effort to transform retailing. Schwab.com is an undertaking intended to redefine the brokerage industry through the use of the Internet. There can be an ROI core or component to analyses of such initiatives, because they often involve major reshaping or reengineering of fundamental organization processes. However, assessing with high degrees of accuracy the ROIs of these initiatives and their related information systems can be very difficult. Several factors contribute to this difficulty:

- These major strategic initiatives usually recast the organization's markets and its roles. The outcome of the recasting, although visionary, can be difficult to see with clarity and certainty.
- The recasting is evolutionary; the organization learns and alters itself as it progresses, over what are often lengthy periods of time. It is difficult to be prescriptive about this evolutionary process. Most integrated delivery systems are confronting this phenomenon.
- Market and competitor responses can be difficult to predict.

IT value is diverse and complex. This diversity indicates the power of IT and the diversity of its use. Nonetheless, the complexity of the value proposition means that it is difficult to make choices between IT investments and also difficult to assess whether the investment ultimately chosen delivered the desired value or not.

The IT Project Proposal

The IT project proposal is a cornerstone in examining value. Clearly, ensuring that all proposals are well crafted does not ensure value. To achieve value, alignment with organization strategies must occur, factors for sustained IT excellence must be managed, budget processes for making choices between investments must exist, and projects must be well managed. However, the proposal (as discussed in Chapter Thirteen) does describe the intended outcome of the IT investment. The proposal requests money and an organizational commitment to devote management attention and staff effort to implementing an information system. The proposal describes why this investment of time, effort, and money is worth it—that is, the proposal describes the value that will result.

In Chapter Thirteen we also discussed budget meetings and management forums that might review IT proposals and determine if a proposal should be accepted. In this section we discuss the value portion of the proposal and some common problems encountered with it.

Sources of Value Information

As project proponents develop their case for an IT investment they may be unsure of the full gamut of potential value or of the degree to which a desired value can be truly realized. The organization may not have had experience with the proposed application and may have insufficient analyst resources to perform its own assessment. It may not be able to answer such questions as, What types of gains have organizations seen as a result of implementing an EMR? To what degree will IT be a major contributor to our efforts to streamline operating room throughput?

Information about potential value can be obtained from several sources (discussed in Appendix A). Conferences often feature presentations that describe the efforts of specific individuals or organizations in accomplishing initiatives of interest to many others. Industry publications may offer relevant articles and analyses. Several industry research organizations—for example, Gartner Group and Forrester—can offer advice. Consultants can be retained who have worked with clients who are facing or have addressed similar questions. Vendors of applications can describe the outcomes experienced by their customers. And colleagues can be contacted to determine the experiences of their organizations.

Garnering an understanding of the results of others is useful but insufficient. It is worth knowing that Organization Y adopted CPOE and reduced unnecessary testing by X percent. However, one must also understand the CPOE features that were critical in achieving that result and the management steps taken and the process changes made in concert with the CPOE implementation.

Formal Financial Analysis

Most proposals should be subjected to formal financial analyses regardless of their value proposition. Several types of financial measures are used by organizations. An organization's finance department will work with leadership to determine which measures will be used and how the measures will be compiled.

Two common financial measures are net present value and internal rate of return:

- *Net present value* is calculated by subtracting the initial investment from the future cash flows that result from the investment. The cash can be generated by new revenue or cost savings. The future cash is discounted, or reduced, by a standard rate to reflect the fact that a dollar earned one or more years from now is worth less than a dollar one has today (the rate depends on the time period considered). If the cash generated exceeds the initial investment by a certain amount or percentage, the organization may conclude that the IT investment is a good one.
- *Internal rate of return* is the discount rate at which the present value of an investment's future cash flow equals the cost of the investment. Another way to look at this is

to ask, Given the amount of the investment and its promised cash, what rate of return am I getting on my investment? On the one hand a return of 1 percent is not a good return (just as one would not think that a 1 percent return on one's savings was good). On the other hand a 30 percent return is very good.

Table 15.1 shows the typical form of a financial analysis for an IT application.

Comparing Different Types of Value

Given the diversity of value, it is very challenging to compare IT proposals that have different value propositions. How does one compare a proposal that promises to increase revenue and improve collaboration to one that offers improved compliance, faster turnaround times, and reduced supply costs?

At the end of the day, judgment is used to choose one proposal over another. Health care executives review the various proposals and associated value statements and make choices based on their sense of organization priorities, available monies, and the likelihood that the value will be seen. These judgments can be aided by the development of a scoring approach that helps the leadership develop a common *metric* across proposals. For example, the organization might decide to score each proposal according to how much value it promises to deliver in each of the following areas:

- Revenue impact
- Cost reduction
- Patient or customer satisfaction
- Quality of work life
- Quality of care
- Regulatory compliance
- Potential learning value

In this approach, each of these areas in each proposal is assigned a score, ranging from 5 (significant contribution to the area) to 1 (minimal or no contribution). The scores are then totaled for each proposal, and in theory, one picks those proposals with the highest aggregate scores. In practice, IT investment decisions are rarely that algorithmic. However, such scoring can be very helpful in sorting through complex and diverse value propositions:

- Scoring forces the leadership team to discuss why different members of the team assigned different scores—why, for example, did one person assign a score of 2 for the revenue impact of one proposal and another assign a 4? These discussions can clarify people's understandings of proposal objectives and help the team arrive at a consensus regarding each project.

TABLE 15.1 FINANCIAL ANALYSIS OF A PATIENT ACCOUNTING DOCUMENT IMAGING SYSTEM.

	Current Year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
COSTS								
One-time capital expense	\$1,497,466	\$1,302,534						
System operations								
System maintenance	-	288,000	\$288,000	\$288,000	\$288,000	\$288,000	\$288,000	\$288,000
System maintenance (PHS)	-	152,256	152,256	152,256	152,256	152,256	152,256	152,256
TOTAL COSTS	1,497,466	1,742,790	440,256	440,256	440,256	440,256	440,256	440,256
BENEFITS								
Revenue gains								
Rebiling of small secondary balances	-	651,000	868,000	868,000	868,000	868,000	868,000	868,000
Medicaid billing documentation	-	225,000	300,000	300,000	300,000	300,000	300,000	300,000
Disallowed Medicare bad debt audit	-	-	-	-	100,000	100,000	100,000	100,000
Staff savings								
Projected staff savings	-	36,508	136,040	156,504	169,065	169,065	169,065	171,096
Operating savings								
Projected operating savings	-	64,382	77,015	218,231	222,550	226,436	226,543	229,935
TOTAL BENEFITS	-	976,891	1,381,055	1,542,735	1,659,615	1,663,502	1,663,608	1,669,031
CASH FLOW	(1,497,466)	(765,899)	940,799	1,102,479	1,219,359	1,223,246	1,223,352	1,228,775
CUMULATIVE CASH FLOW	(1,497,466)	(2,263,365)	(1,322,566)	(220,087)	999,272	2,222,517	3,445,869	4,674,644
NPV (12% discount)	1,998,068							
IRR			33%					

- Scoring means that the leadership team will have to defend any decision not to fund a project with a high score or to fund one with a low score. In the latter case, team members will have to discuss why they are all in favor of a project when it has such a low score.

The organization can decide which proposal areas to score and which not to score. Some organizations give different areas different weights—for example, reducing costs might be considered twice as important as improving organizational learning. The resulting scores are not binding, but they can be helpful in arriving at a decision about which projects will be approved and what value is being sought. (A form of this scoring process was displayed earlier in Figure 12.5.)

Tactics for Reducing the Budget

Proposals for IT initiatives may originate from a wide variety of sources in an organization. The IT group will submit proposals as will department directors and physicians. Many of these proposals will not be directly related to an overall strategy, but they can nevertheless be “good ideas” that if implemented would lead to improved organizational performance. So it is common for an organization to have more proposals than it can fund. For example, during the IT budget discussion the leadership team may decide that although it is looking at \$2.2 million in requests, the organization can afford to spend only \$1.7 million, so \$500,000 worth of requests must be denied. Table 15.2 presents a sample list of requests.

Reducing the budget in situations like this requires a value discussion. The leadership is declaring some initiatives to have more value than others. Scoring initiatives according to criteria is one approach to addressing this challenge.

In addition to such scoring, other assessment tactics can be employed, prior to the scoring, that can assist the leadership in making reduction decisions.

- Some requests are *mandatory*. They may be mandatory because of a regulation requirement (such as the HIPAA Security Rule) or because a current system is so obsolete that it is in danger of crashing—permanently—and it must be replaced soon. These requests must be funded.
- Some projects can be delayed. They are worthwhile, but a decision on them can be put off until next year. The requester will get by in the meantime.
- Key groups within IT, such as the staff who manage clinical information systems, may already have so much on their plate that they cannot possibly take on another project. Although the organization wants to do the project, it would be ill advised to do so now, and so the project can be deferred to next year.
- The user department proposing the application may not have strong management or may be experiencing some upheaval; hence implementing a new system at this

**TABLE 15.2. REQUESTS FOR NEW INFORMATION
SYSTEM PROJECTS.**

Community General Hospital	
Project Name	Operating Cost
TOTAL	\$2,222,704
Clinical portfolio development	38,716
Enterprise monitoring	70,133
HIPAA security initiative	36,950
Accounting of disclosure—HIPAA	35,126
Ambulatory Center patient tracking	62,841
Bar-coding infrastructure	62,841
Capacity management	155,922
Chart tracking	34,876
Clinical data repository—patient care information system (PCIS) retirement	139,902
CRP research facility	77,026
Emergency Department data warehouse	261,584
Emergency Department order entry	182,412
Medication administration system	315,323
Order communications	377,228
Transfusion services replacement system	89,772
Wireless infrastructure	44,886
Next generation order entry	73,403
Graduate medical education duty hours	163,763

time would be risky. The project could be denied or delayed until the management issues have been resolved.

- The value proposition or the resource estimates, or both, are shaky. The leadership team does not trust the proposal, so it could be denied or sent back for further analysis. Further analysis means that the proposal will be examined next year.
- Less expensive ways may exist of addressing the problems cited in the proposal. These ways may involve a less expensive application or a non-IT approach. The proposal could be sent back for further analysis.
- The proposal is valuable, and the leadership team would like to move it forward. However, it may reduce the budget, enabling progress to occur but at a slower pace. This delays the value but ensures that resources are devoted to making progress.

These tactics are routinely employed during budget discussions aimed at trying to get as much value as possible given finite resources.

Common Proposal Problems

During the review of IT investment proposals, organizational leadership might encounter several problems related to the estimates of value and the estimates of the resources needed to obtain the value. If undetected, these problems might lead to a significant overstatement of potential return. An overstatement, obviously, may result in significant organizational unhappiness when the value that people thought they would see never materializes and never could have materialized.

Fractions of Effort. Proposal analyses might indicate that the new IT initiative will save fractions of staff time, for example, that each nurse will spend fifteen minutes less per shift on clerical tasks. To suggest a total value, the proposal might multiply (and this formula is simplistic): 200 nurses x 15 minutes saved per 8-hour shift x 250 shifts worked per year = 12,500 hours saved. The math might be correct, and the conclusion that 12,500 hours will become available for doing other work such as direct patient care might be correct. But the analysis will be incorrect if it then concludes that the organization could now “save” the salary dollars of six nurses (assuming 2,000 hours worked per year per nurse).

Saving fractions of staff effort does not always lead to salary savings, even when there are large numbers of staff, because there may be no practical way to lay off six nurses. If, for example, there are six nurses working each 8-hour shift in a particular nursing unit, the 15 minutes saved per nurse would lead to a total savings of 1.5 hours per shift. But if one were then to lay off one nurse on a shift, it would reduce the nursing capacity on that shift by 8 hours, damaging the unit’s ability to deliver care. Saving fractions of staff effort also does not lead to salary savings when staff are geographically highly fragmented or when they work in small units or teams. It leads to possible salary savings only when staff work in very large groups and the work of the reduced staff can be redistributed to others.

Reliance on Complex Behavior. Proposals may project with great certainty that people will use systems in specific ways. For example, several organizations expect that consumers will use Internet-based quality report cards to choose their physicians and hospitals. However, few consumers actually rely on such sites. Organizations can expect that nurses will readily adopt systems that help them discharge patients faster. However, nurses often delay entering discharge transactions so that they can grab a moment of peace in an otherwise overwhelmingly busy day.

System use is often not what was anticipated. This is particularly true when the organization has no experience with a class of users or with the introduction of IT into certain types of tasks. The original value projection can be thrown off by the

complex behaviors of system users. People do not always behave as we expect or want them to. If user behavior is uncertain, the organization would be wise to pilot an application and learn from this demonstration.

Unwarranted Optimism. Project proponents are often guilty of optimism that reflects a departure from reality. Proponents may be guilty of any of four mistakes:

- They assume that nothing will go wrong with the project.
- They assume that they are in full control of all variables that might affect the project—even, for example, quality of vendor products and organizational politics.
- They believe that they know exactly what changes in work processes will be needed and what system features must be present, when what they really have, at best, are close approximations of what must happen.
- They believe that everyone can give full time to the project and forget that people get sick or have babies and that distracting problems unrelated to the project will occur, such as a sudden deterioration in the organization's fiscal performance, and demand attention.

This optimism results in project budgets and timetables being overrun and compromises in system goals being necessary. Overruns and compromises change the value proposition.

Shaky Extrapolations. Projects often achieve gains in the first year of their implementation, and proponents are quick to project that such gains will continue to be made during the remaining life of the project. For example, an organization may see 10 percent of its physicians move from using dictation when developing a progress note to using structured, computer-based templates. The organization might erroneously extrapolate that each year will see an additional 10 percent shift. In fact the first year might be the only year in which such a gain will occur. The organization has merely convinced the more computer facile physicians to change, and the rest of the physicians have no interest in ever changing.

Phantom Square Feet. Project proposals often state that the movement to digital records removes or reduces the need for space to house paper records. At the least, they say, the paper records could be moved off site. This in turn can lead to the claim that the money once spent on that space—for example, \$40 per square foot—can be considered a fiscal return. In fact, such space “savings” occur only when the building of new space (for any purpose) does not occur because the organization used the freed-up records space instead. Space, like labor, represents a savings only when reducing the need for it truly does prevent further expenditure on space. If the organization uses

the freed-up space but never had any intention of spending money to build more space, then any apparent savings are phantom savings.

Underestimating the Effort. Project proposals might count the IT staff effort in the estimates of project costs but not count the time that users and management will have to devote to the project. A patient care system proposal, for instance, may not include the time that will be spent by dozens of nurses working on system design, developing workflow changes, and attending training. These efforts are real costs. They often lead to the need to hire temporary nurses to provide coverage on the inpatient care units, or they might lead to a reduced patient census because there are fewer nursing hours available for patient care. Such miscounting of effort understates the cost of the project.

Fairy-Tale Savings. IT project proposals may note that the project can reduce the expenses of a department or function, including costs for staff, supplies, and effort devoted to correcting mistakes that occur with paper-based processes. Department managers will swear in project approval forums that such savings are real. However, when asked if they will reduce their budgets to reflect the savings that will occur, these same managers may become significantly less convinced that the savings will result. They may comment that the freed-up staff effort or supplies budgets can be redeployed to other tasks or expenses. The managers may be right that the expenses should be redeployed, and all managers are nervous when asked to reduce their budgets and still do the same amount of work. However, the savings expected have now disappeared.

Failure to Account for Postimplementation Costs. After a system goes live the costs of the system do not go away. System maintenance contracts are necessary. Hardware upgrades will be required. Staff may be needed to provide enhancements to the application. These support costs may not be as large as the costs of implementation. But they are costs that will be incurred every year, and over the course of several years, they can add up to some big numbers. Proposals often fail to adequately account for support costs.

Steps to Improve Value Realization

Achieving value from IT investments requires management effort. There is no computer genie that descends upon the organization once the system is live and waves its wand and—shazzam!—value has occurred. Achieving value is hard work but doable work. Management can take several steps to realize value (Dragoon, 2003; Glaser, 2003a, 2003b). These steps are discussed in the sections that follow.

Make Sure That the Homework Was Done

IT investment decisions are often made based on proposals that are not resting on solid ground. The proposer has not done the necessary homework, and this elevates the risk of a suboptimal return.

Clearly, the track record of the investment proposer will have a significant influence on the likelihood that a favorable investment decision will be made and that the resulting investment will deliver value. However, regardless of the proposer's track record, an IT proposal should enable the leadership team to respond with a strong yes to each of the following questions:

- Is it clear how the plan advances the organization's strategy?
- Is it clear how care will improve, costs will be reduced, or service will be improved? Are the measures of current performance and expected improvement well researched and realistic? Have the related changes in operations, workflow, and organization processes been defined?
- Are the senior leaders whose areas are the focus of the IT plan clearly supportive? Could they give the presentation?
- Are the resource requirements well understood and convincingly presented? Have these requirements been compared to those experienced by other organizations undertaking similar initiatives?
- Have the investment risks been identified, and is there an approach to addressing these risks?
- Do we have the right people assigned to the project, have we freed up their time, and are they well organized?

Answering with a no, a maybe, or an equivocal yes to any of these questions should lead one to believe that the discussion is perhaps focusing on an expense rather than an investment.

Require Formal Project Proposals

It is a fact of organizational life that projects are approved as a result of hallway conversations or discussions on the golf course. Organizational life is a political life. While recognizing that reality, the organization should require that every IT project be written up in the format of a proposal and that each proposal should be reviewed and subjected to scrutiny before the organization will commit to supporting the initiative. However, an organization may also decide that small projects—for example, those that involve less than \$25,000 in costs and less than 120 person-hours—can be handled more informally.

Increase Accountability for Investment Results

Few meaningful organization initiatives are accomplished without establishing appropriate accountability for results. Accountability for IT investment results can be improved by taking three major steps.

First, the business owner of the IT investment should defend the investment—for example, the director of clinical laboratories should defend the request for a new laboratory system and the director of nursing should defend the need for a new nursing system. The IT staff will need to work with the business owner to define IT costs, establish likely implementation time frames, and sort through application alternatives. The IT staff should never defend an application investment.

Second, as was discussed in Chapter Fourteen, project sponsors and business owners must be defined, and they must understand the accountability that they now have for the successful completion of the project.

Third, the presentation of these projects should occur in a forum that routinely reviews such requests. Seeing many proposals, and their results, over the course of time will enable the forum participants to develop a seasoned understanding of good versus not-so-good proposals. The forum is also able to compare and contrast proposals as it decides which ones should be approved. A manager might wonder (and it's a good question), "If I approve this proposal, does that mean that we won't have resources for another project that I might like even better?" Examining as many proposals together as possible enables the organization to take a portfolio view of its potential investments.

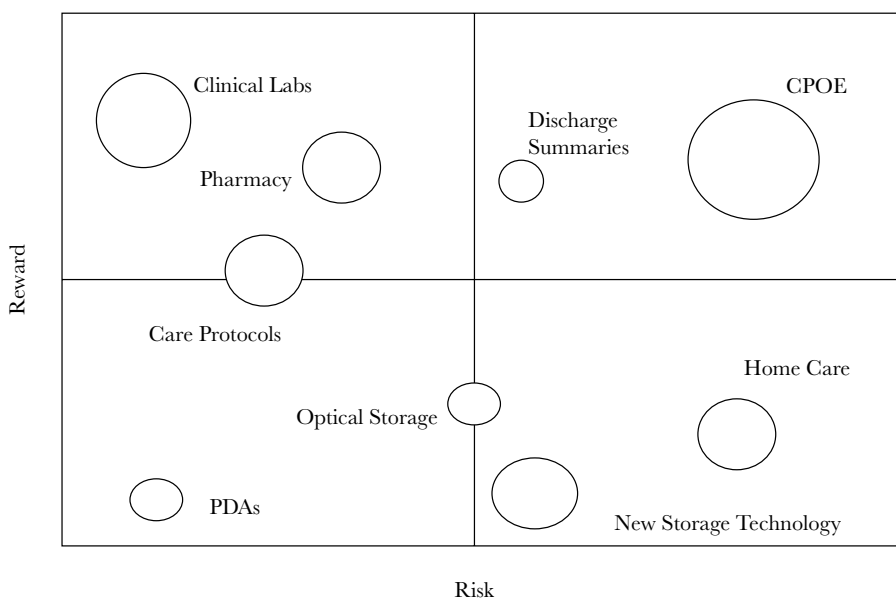
Figure 15.1 displays an example of a project investment portfolio represented graphically. The size of each bubble reflects the magnitude of a particular IT investment. The axes are labeled "reward" (the size of the expected value) and "risk" (the relative risk that the project will not deliver the value). Other axes may be used. One commonly used set of axes consists of "support of operations" and "support of strategic initiatives."

Diagrams such as this serve several functions:

- They summarize IT activity on one piece of paper, allowing the leadership to consider a new request in the context of prior commitments.
- They help to ensure a balanced portfolio, promptly revealing imbalances such as a clustering of projects in the high-risk quadrant.
- They help to ensure that the approved projects cover an appropriate spectrum of organizational needs—for example, that projects are directed to revenue cycle improvement, to operational improvement, and to patient safety.

Conduct Postimplementation Audits

Rarely do organizations revisit their IT investments to determine if the promised value was actually achieved. Organizations believe that once the implementation is over and the change settles in, value will have been automatically achieved. This is unlikely.

FIGURE 15.1. IT INVESTMENT PORTFOLIO.

Source: Adapted from Arlotto and Oakes, 2003.

Postimplementation audits can be conducted to identify value achievement progress and the steps still needed to achieve maximum gain. An organization might decide to audit two to four systems each year, selecting systems that have been live for at least six months. During the course of the audit meeting, these five questions can be asked:

1. What goals were expected at the time the project investment was approved?
2. How close have we come to achieving those original goals?
3. What do we need to do to close the goal gap?
4. How much have we invested in the implementation of the system, and how does that compare to our original budget?
5. If we had to implement this system again, what would we do differently?

Postimplementation audits assist value achievement by

- Signaling leadership interest in ensuring the delivery of results
- Identifying steps that still need to be taken to ensure value

- Supporting organizational learning about IT value realization
- Reinforcing accountability for results

Celebrate Value Achievement

Business value should be celebrated. Organizations usually hold parties shortly after applications go live. These parties are appropriate; a lot of people worked very hard to get the system up and running and used. However, up and running and used does not mean that value has been delivered. In addition to go-live parties, organizations should consider business value parties; celebrations conducted once the value has been achieved—for example, a party that celebrates the achievement of service improvement goals. Go-live parties alone risk sending the inappropriate signal that implementation is the end point of the IT initiative. Value delivery is the end point.

Leverage Organizational Governance

The creation of an IT committee of the board of directors can enhance organizational efforts to achieve value from IT investments. At times the leadership team of an organization is uncomfortable with some or all of the IT conversation. Team members may not understand why infrastructure is so expensive or why large implementations can take so long and cost so much. They may feel uncomfortable with the complexity of determining the likely value to be obtained from IT investments. The creation of a subcommittee made up of the board members most experienced with such discussions can help to ensure that hard questions are being asked and that the answers are sound.

Shorten the Cycle of Deliverables

When possible, projects should have short deliverable cycles. In other words, rather than asking the organization to wait twelve or eighteen months to see the first fruits of its application implementation labors, make an effort to deliver a sequence of smaller implementations. For example, one might conduct pilots of an application in a subset of the organization, followed by a staged rollout. Or one might plan for serial implementation of the first 25 percent of the application features.

Pilots, staged rollouts, and serial implementations are not always doable. Where they are possible, however, they enable the organization to achieve some value earlier rather than later, support organizational learning about which system capabilities are really important and which were only thought to be important, facilitate the development of reengineered operational processes, and create the appearance (whose importance is not to be underestimated) of more value delivery.

Benchmark Value

Organizations should benchmark their performance in achieving value against the performance of their peers. These benchmarks might focus on process performance—for example, days in accounts receivables or average time to get an appointment. An important aspect of value benchmarking is the identification of the critical IT application capabilities and related operational changes that enabled the achievement of superior results. This understanding of how other organizations achieved superior IT-enabled performance can guide an organization's efforts to continuously achieve as much value as possible from its IT investments.

Communicate Value

Once a year the information technology department should develop a communication plan for the twelve months ahead. This plan should indicate which presentations will be made in which forums and how often IT-centric columns will appear in organizational newsletters. The plan should list three or so major themes—for example, specific Internet strategies or efforts to improve IT service—that will be the focus of these communications. Communication plans try to remedy the fact that even when value is being delivered the organization may not be fully aware of it.

Why IT Investment Fails to Deliver Returns

It is not uncommon to hear leaders of health care organizations complain about the lack of value obtained from IT investments. These leaders may see IT as a necessary expense that must be tightly controlled rather than as an investment that can be a true enabler. New health care managers often walk into organizations where the leadership mind-set features this set of conclusions:

The magnitude of the organization's IT operating and capital budgets is large. IT operating costs may consume 3 percent of the total operating budget, and IT capital may claim 15 to 30 percent of all capital. Although 3 percent may appear small, it can be the difference between a negative operating margin and a positive margin. A 15 to 30 percent IT consumption of capital invariably means that funding for biomedical equipment (which can mean new revenue) and buildings (which improve the patient and staff friendliness of the organization and support the growth of clinical services) is diminished. IT can be seen as taking money away from “worthwhile initiatives.”

The projected growth in IT budgets exceeds the growth in other budget categories. Provider organizations may permit overall operating budgets to increase at a rate close to the inflation rate (3 to 4 percent). However, expenditures on IT often experience growth rates of 10 to 15 percent. At some point an organization will note that the IT budget growth rate may single-handedly lead to insolvency.

Regardless of the amount spent, the leadership feels that not enough is being spent. Worthwhile proposals go unfunded every year. Infrastructure replacement and upgrades seem never ending: “I thought we upgraded our network two years ago. Are you back already?”

It is difficult to evaluate IT capital requests. At times this difficulty is a reflection of a poorly written or fatuous proposal. However, it can be genuinely difficult to compare a proposal directed at improving service to one directed at improving care quality to one directed at increasing revenue to one needed to achieve some level of regulatory compliance.

When asked to “list three instances over the last five years where IT investments have resulted in clear and unarguable returns to the organization,” leaders may return blank stares. However, the conversation may be difficult to stop when they are asked to “list three major IT investment disappointments that have occurred over the last five years.”

If the value from information technology can be significant, why does one hear these management concerns? There are several reasons why IT investments become simply IT expenses. The organization

- Does not establish a clear linkage between IT investments and organization strategy
- Asks the wrong question
- Conducts the wrong analysis
- Does not state its investment goals
- Does not manage outcomes
- Leaps to an inappropriate solution
- Mangles the project management
- Has not learned from studies of IT effectiveness

The Organization Does Not Establish a Clear Linkage Between IT Investments and Organization Strategy

The linkage between IT investments and the organization’s strategy was discussed in Chapter Twelve. When strategies and investments are not aligned, even if the IT department is executing well, it may be working on the wrong things or trying to support a flawed overall organization strategy.

Linkage failures can occur because

- The organization strategy is no more than a slogan or a buzzword with the depth of a bumper sticker, making any investment toward achieving it ill considered.
- The IT department thinks it understands the strategy but it does not, resulting in an implementation of an IT version of the strategy rather than the organization’s version
- The strategists (for a variety of reasons) will not engage in the IT discussion, forcing IT leaders to be mind readers.

- The linkage is superficial—for example, “Patient care systems can reduce nursing labor costs but we haven’t thought through how that will happen.”
- The IT strategy conversation is separated from the organization strategy conversation as a result of the creation of an information systems steering committee, for example—reducing the likelihood of alignment.
- The organization strategy evolves faster than IT can respond.

The Organization Asks the Wrong Question

Rarely should one ask the question, What is the ROI of a computer system? This question makes as much sense as the question, What is the ROI of a chain saw? If one wants to make a dress, a chain saw is a waste of money. If one wants to cut down some trees, one can begin to think about the return on a chain saw investment. One will want to compare that investment to other investments, such as an investment in an ax. One will also want to consider the user. If the chain saw is to be used by a ten-year-old child, the investment might be ill advised. If the chain saw is to be used by a skilled lumberjack, the investment might be worth it.

An organization can determine the ROI of an investment in a tool only if it knows the task to be performed and the skill level of the participants who are to perform the task. Moreover, a positive ROI is not an inherent property of an IT investment. The organization has to manage a return into existence.

Hence, instead of asking, What is the ROI of a computer system? the leadership team members should ask questions such as these:

- What are the steps and investments, including IT steps and investments, that we need to take or make in order to achieve our goals?
- Which business manager owns the achievement of these goals? Does this person have our confidence?
- Do the cost, risk, and time frame associated with the implementation of this set of investments, including the IT investment, seem appropriate given our goals?
- Have we assessed the trade-offs and opportunity costs?
- Are we comfortable with our ability to execute?

The Organization Conducts the Wrong Analysis

There are times when determining ROI is the appropriate investment analysis technique. If a set of investments is intended to reduce clerical staff, an ROI can be calculated. However, there are times when an ROI calculation is clearly inappropriate. What is the ROI of software that supports collaboration? One could calculate the ROI,

but it is hard to imagine an organization basing its investment decision on that analysis. Would an ROI analysis have captured the strategic value of the Amazon.com system or the value of automated teller machines? Few strategic IT investments have impacts that are fully captured by an ROI analysis. Moreover, strategic impact is rarely fully understood until years after implementation. Whatever ROI analysis might have been done would have invariably been wrong.

As was discussed earlier, the objective of the IT investment points to the appropriate approach to the analysis of its return. Sometimes organizations apply financial techniques such as internal rate of return in a manner that is overzealous and ignores other analysis approaches. This misapplication of technique can clearly lead to highly worthwhile initiatives being deemed unworthy of funding.

The Organization Does Not State Its Investment Goals

Statements about the positive contributions that the investment will make to organizational performance often accompany IT proposals. But the proposals are not always accompanied by specific numerical goals for this improvement. If we intend to reduce medical errors, will we reduce errors by 50 percent or 80 percent or some other number? If we intend to reduce claims denials, will we reduce them to 5 percent or 2 percent, and how much revenue will be realized as a result of this reduction?

Failure to be numerically explicit about goals can create three fundamental value problems.

The organization may not know how well it performs now. If the current error rate or denial rate is not known, it is hard to believe that the leadership has studied the problem well enough to be fairly sure that an IT investment will help achieve the desired gains. The IT proposal sounds more like a guess about what is needed.

The organization may never know whether it got the desired value or not. If the proposal does not state a goal, the organization will never know whether the 20 percent reduction in errors it has achieved is as far as it can go or whether it is only halfway to its desired goal. It does not know whether it should continue to work on the error problem or whether it should move on to the next performance issue.

It will be difficult to hold someone accountable for performance improvement when the organization is unable to track how well he or she is doing.

The Organization Does Not Manage Outcomes

Related to the failure to state goals is the failure to manage outcomes into existence. Once the project is approved and the system is up, management goes off to the next challenge seemingly unaware that the work of value realization has just begun.

Figure 15.2 depicts a reduction in days in accounts receivable (AR) at a Partners HealthCare System physician practice. During the interval depicted, a new practice management system was implemented. The practice did not see a precipitous decline in days in AR (a sign of improved revenue performance) in the time immediately following the implementation in the second quarter of 1997. The practice did see a progressive improvement in days in AR because someone was managing that improvement.

If the gain in revenue performance had been an “automatic” result of the information system implementation, the practice would have seen a very sharp drop in days in AR. Instead it saw a gradual improvement over time. This gradual change reflects that

- The gain occurred through day in, day out changes in operational processes, fine-tuning of system capabilities, and follow-ups in staff training.
- A person had to be in charge of obtaining this improvement. Someone had to identify and make operational changes, manage changes in system capabilities, and ensure that needed training occurred.

The Organization Leaps to an Inappropriate Solution

At times the IT discussion of a new application succumbs to advanced states of technical arousal. Project participants become overwhelmed by the prospect of using sexy new technology and state-of-the-art gizmos and lose their senses and understanding of why they are having this discussion in the first place. Sexiness and state-of-the-art-ness become the criteria for making system decisions.

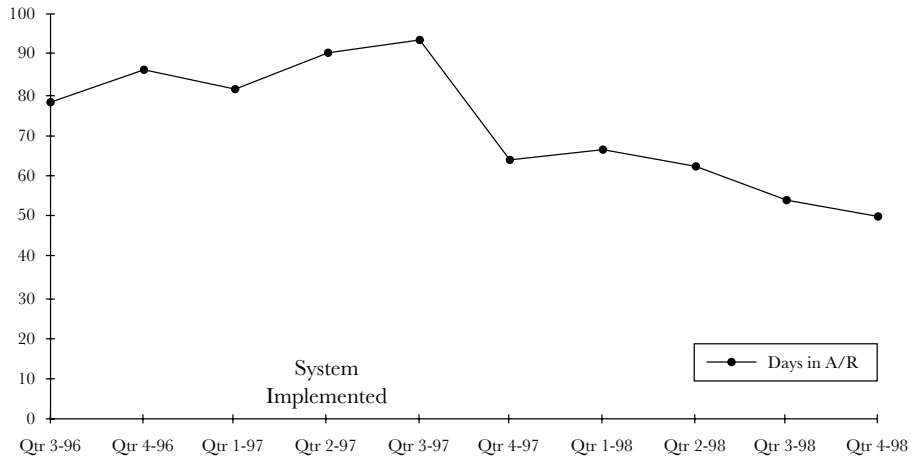
In addition the comparison of two alternative vendor products can turn into a features war. The discussion may focus on the number of features as a way of distinguishing products and fail to ask whether this numerical difference has any real impact on the value that is desired.

Both sexiness and features have their place in the system selection decision. However, they are secondary to the discussion that centers on the capabilities needed to affect specific performance goals. Sexiness and features may be irrelevant to the performance improvement discussion.

The Organization Mangles the Project Management

One guaranteed way to reduce value is to mangle the management of the implementation project. Implementation failures or significant budget and timetable overruns or really unhappy users, any of these can dilute value.

FIGURE 15.2. DAYS IN ACCOUNTS RECEIVABLE BEFORE AND AFTER IMPLEMENTATION OF PRACTICE MANAGEMENT SYSTEM.



Among the many factors that can lead to mangled project management are these:

- The project's scope is poorly defined.
- The accountability is unclear.
- The project participants are marginally skilled.
- The magnitude of the task is underestimated.
- Users feel like victims rather than participants.
- All the world has a vote and can vote at any time.

Many of these factors were discussed in Chapters Seven and Fourteen.

The Organization Has Not Learned from Studies of IT Effectiveness

Organizations may fail to invest in the IT abilities discussed in Chapter Thirteen, such as good relationships between the IT function and the rest of the organization and a well-architected infrastructure. This investment failure increases the likelihood that the percentage of projects that fail to deliver value will be higher than it should be.

Analyses of the IT Value Challenge

The IT investment and value challenge plagues all industries. It is not a problem peculiar to health care. The challenge has been with us for forty years, ever since organizations began to spend money on big mainframes. This challenge is complex and persistent, and we should not believe that we can fully solve it. We should believe that we can be better at dealing with it. This section highlights the conclusions of several studies and articles that have examined this challenge.

Factors That Hinder Value Return

The study by the Committee to Study the Impact of Information Technology on the Performance of Service Activities (1994) found these major contributors to failures to achieve a solid return on IT investments:

- The organization's overall strategy is wrong, or its assessment of its competitive environment is inadequate.
- The strategy is fine, but the necessary IT applications and infrastructure are not defined appropriately. The information system, if it is solving a problem, is solving the wrong problem.
- The organization fails to identify and draw together well all the investments and initiatives necessary to carry out its plans. The IT investment then falters because other changes, such as reorganization or reengineering, fail to occur.
- The organization fails to execute the IT plan well. Poor planning or less than stellar management can diminish the return from any investment.

Value may also be diluted by factors outside the organization's control. Weill and Broadbent (1998) noted that the more strategic the IT investment, the more its value can be diluted. An IT investment directed to increasing market share may have its value diluted by non-IT decisions and events—for example, pricing decisions, competitors' actions, and customers' reactions. IT investments that are less strategic but have business value—for example, improving nursing productivity—may be diluted by outside factors—for example, shortages of nursing staff. And the value of an IT investment directed toward improving the characteristics of the infrastructure may be diluted by outside factors—for example, unanticipated technology immaturity or business difficulties confronting a vendor.

The Relationship Between IT Investment and Organizational Performance

A study by Strassmann (1990) examined the relationship between IT expenditures and organizational effectiveness. Data from an *Information Week* survey of the top 100 users of information technology were used to correlate IT expenditures per employee

with profits per employee. Strassmann concluded that there is no obvious direct relationship between expenditure and organizational performance. This finding has been observed in several other studies (for example, Keen, 1997). It leads to several conclusions:

- Spending more on IT is no guarantee that the organization will be better off. There has never been a direct correlation between spending and outcomes. Paying more for care does not give one better care. Clearly, one can spend so little that nothing effective can be done. And one can spend so much that waste is guaranteed. But moving IT expenditures from 2 percent of the operating budget to 3 percent of the operating budget does not inherently lead to a 50 percent increase in desirable outcomes.
- Information technology is a tool, and its utility as a tool is largely determined by the tool user and his or her task. Spending a large amount of money on a chain saw for someone who doesn't know how to use one is a waste. Spending more money for tools for the casual saw user who trims an apple tree every now and then is also a waste. However, skilled loggers might say that if a chain saw blade were longer and the saw's engine more powerful, they would be able to cut 10 percent more trees in a given period of time. The investment needed to enhance the loggers' saws might lead to superior performance. Organizational effectiveness in applying IT has an enormous effect on the likelihood of a useful outcome from increased IT investment.
- Factors other than the appropriateness of the tool to the task also influence the relationship between IT investment and organizational performance. These factors include the nature of the work (for example, IT is likely to have a greater impact on bank performance than on consulting firm performance), the basis of competition in an industry (for example, cost per unit of manufactured output versus prowess in marketing), and an organization's relative competitive position in the market.

The Value of the Overall IT Investment

Many analyses and academic studies have been directed to answering this broad question, How can an organization assess the value of its overall investments in IT? Assessing the value of the aggregate IT investment is different from assessing the value of a single initiative or other specific investment. And it is also different from assessing the caliber of the IT department. Developing a definitive, accurate, and well-accepted way to answer this question has so far eluded all industries and may continue to be elusive. Nonetheless there are some basic questions that can be asked in pursuit of answering the larger question. Interpreting the answers to these basic questions is a subjective exercise, making it difficult to derive numerical scores. Bresnahan (1998) suggests five questions:

1. How does IT influence the customer experience?
2. Do patients and physicians, for example, find that organizational processes are more efficient, less error prone, and more convenient?
3. Does IT enable or retard growth? Can the IT organization support effectively the demands of a merger? Can IT support the creation of clinical product lines—for example, cardiology—across the IDS?
4. Does IT favorably affect productivity?
5. Does IT advance organizational innovation and learning?

IT as a Commodity

Carr (2003) has equated IT with commodities—soy beans, for example. Carr's argument is that core information technologies, such as fast, inexpensive processors and storage, are readily available to all organizations and hence cannot provide a competitive advantage. Organizations can no more achieve value from IT than an automobile manufacturer can achieve value by buying better steel than a competitor does or a grocer can achieve value by stocking better sugar than a competitor does. In this view, IT, steel, and sugar are all commodities.

Responding to Carr's argument, Brown and Hagel (2003) make three observations about IT value:

1. "Extracting value from IT requires innovation in business practices." If an organization merely computerizes existing processes without rectifying (or at times eliminating) process problems, it may have merely made process problems occur faster. In addition those processes are now more expensive because there is a computer system to support. Providing appointment scheduling systems may not make waiting times any shorter or enhance patients' ability to get an appointment when they need one.

All IT initiatives should be accompanied by efforts to materially improve the processes that the system is designed to support. IT often enables the organization to think differently about a process or expand its options for improving a process. If the process thinking is too narrow or too unimaginative, the value that could have been achieved will have been lost, with the organization settling for an expensive way to achieve minimal gain. For example, if Amazon.com had thought that the Internet enabled it to simply replace the catalogue and telephone as a way of ordering something, it would have missed ideas such as presenting products to the customer based on data about prior orders or enabling customers to leave their own ratings of books and music.

2. "IT's economic impact comes from incremental innovations rather than from 'big bang' initiatives." Organizations will often introduce very large computer systems and process change "all at once." Two examples of such big bangs are the replacement of all systems related to the revenue cycle and the introduction of a new patient care system over the course of a few weeks.

Big bang implementations are very tricky and highly risky. They may be haunted by series of technical problems. Moreover, these systems introduce an enormous number of process changes affecting many people. It is exceptionally difficult to understand the ramifications of such change during the analysis and design stages that precede implementation. A full understanding is impossible. As a result, the implementing organization risks material damage. This damage destroys value. It may set the organization back, and even if the organization grinds its way through the disruption, the resulting trauma may make the organization unwilling to engage in future ambitious IT initiatives. In contrast, IT implementations (and related process changes) that are more incremental and iterative reduce the risk of organizational damage and permit the organization to learn. The organization has time to understand the value impact of phase n and then can alter its course before it embarks upon phase $n + 1$. Moreover, incremental change leads the organization's members to understand that change, and realizing value, are a never ending aspect of organizational life rather than something to be endured every couple of years.

3. "The strategic impact of IT investments comes from the cumulative effect of sustained initiatives to innovate business practices in the near term." If economic value is derived from a series of thoughtful, incremental steps, then the aggregate effect of those steps should be a competitive advantage. Most of the time, organizations that wind up dominating an industry do so through incremental movement over the course of several years (Collins, 2001). This observation is consistent with our view in Chapter Twelve. Persistent innovation by a talented team, over the course of years, will result in significant strategic gains. The organization has learned how to improve itself, year in and year out. Strategic value is a marathon. It is a long race that is run and won one mile at a time.

Summary

IT value is complex, multifaceted, and diverse across and within proposed initiatives. The techniques used to analyze value must vary with the nature of the value.

The project proposal is the core means for assessing the potential value of a potential IT initiative. IT proposals have a commonly accepted structure. And approaches exist for comparing proposals with different types of value propositions. Project proposals often present problems in the way they estimate value—for example, they may unrealistically combine fractions of effort saved, fail to appreciate the complex behavior of system users, or underestimate the full costs of the project.

Many factors can dilute the value realized from an IT investment. Poor linkage between the IT agenda and the organization strategy, the failure to set goals, and the failure to manage the realization of value all contribute to dilution.

There are steps that can be taken to improve the achievement of IT value. Leadership can ensure that project proponents have done their homework, that accountability for results has been established, that formal proposals are used, and that postimplementation audits are conducted. Even though there are many approaches and factors that can enhance the realization of IT-enabled value, the challenges of achieving this value will remain a management issue for the foreseeable future.

Health care organization leadership often feels ill equipped to address the IT investment and value challenge. However, no new management techniques are required to evaluate IT plans, proposals, and progress. Leadership teams are often asked to make decisions that involve strategic hunches (such as a belief that developing a continuum of care would be of value) about areas where they may have limited domain knowledge (new surgical modalities) and where the value is fuzzy (improved morale). Organizational leaders should treat IT investments just as they would treat other types of investments; if they don't understand, believe, or trust the proposal, or its proponent, they shouldn't approve it.

Chapter Fifteen: Learning Activities

1. Interview the CIO of a local provider or payer. Discuss how his or her organization assesses the value of IT investments and ensures that the value is delivered.
2. Select two articles from a health care IT trade journal that describe the value an organization received from its IT investments. Critique and compare the articles.
3. Select two examples of intangible value. Propose one or more approaches that an organization might use to measure each of those values.
4. Prepare a defense of the value of a significant investment in an electronic medical record system.



APPENDIX A

OVERVIEW OF THE HEALTH CARE IT INDUSTRY

There is a health care information technology industry. This industry is composed of companies that provide hardware, software, and a wide range of services, including consulting and outsourcing, to health care organizations. The industry also includes associations that support the professional advancement of the health care IT professional, organizations that put on industry conferences, and publications that cover current topics and issues in the industry.

It is not possible to develop an IT strategy and implement that strategy without engaging this industry.

This Appendix provides an overview of this industry. It will discuss

- The size, structure, and composition of the health care IT industry, and characteristics of health care that affect the application of IT products and services
- Sources of information about that industry
- Health care IT associations

The Health Care IT Industry

Health care is the largest sector of the U.S. economy (\$1.7 trillion in 2003). It is not surprising that a large, diverse, and robust industry has developed to provide IT products and services to that sector. The health care IT industry is generally viewed as

having three major markets; health care providers, health care insurance companies, and health care suppliers—for example, pharmaceutical companies, medical supply distribution companies, and health care device manufacturers. Some industry analyses cover the global health care IT market, and others focus on the market in the United States. We will focus on the health care provider market in the United States.

Size of the Industry

In 2003, health care providers spent \$38.6 billion on IT hardware, software, and services (Cruz, 2003). This spending is expected to increase at a 7 percent compounded annual growth rate for the next several years. Health care was the second fastest growing IT market in 2003; government was the first. (In part, health care's ranking reflects the fact that in 2003 industries such as manufacturing and retail were still recovering from a recession and had slowed their IT spending.) In general, growth in IT spending among health care providers is attributed to providers' pursuing IT "answers" to a range of challenges and issues facing them:

- Concerns over patient safety can lead to investments in CPOE and medical administration record systems.
- Problems with shortages of health care professionals and cost pressures can result in efforts to use IT to improve operational efficiency and reduce staff workloads.
- Compliance with new health care regulations, such as rules designed to improve the security of information systems or reduce fraudulent billing, often requires an IT response.
- Desires to improve patient service can lead to new systems designed to improve the process of obtaining an appointment or to reduce test result turnaround time.

Such answers are identified during the IT strategy and alignment process that was discussed in Chapter Twelve.

The typical health care provider's IT spending is proportioned across the categories listed in Table A.1.

Health Care IT Spending Relative to Other Industries

Health care organizations will spend, on average, about 2.5 percent of their revenues on IT. This spending includes the cost of internal IT staff and the cost of purchasing products and services from the market. Across all industries the average is 3.9 percent of revenues spent on IT (Cruz, 2003). In health care, IT employees constitute 4.3 percent of all employees, whereas the cross-industry average is 6.8 percent (Cruz, 2003).

TABLE A.1. TYPICAL PROVIDER DISTRIBUTION OF IT SPENDING.

Expenditure Category	Percentage of IT Spending
Hardware	10
Software	10
Telecommunications ^a	20
Services ^b	40
Internal staff	20

^a Networks, Internet connections, and telephone costs.

^b Implementation, consulting, and product maintenance services.

Source: Cruz, 2003.

Why does health care have this apparently lower level of IT spending? To some degree the percentages reflect the cost structure of health care. Being a health care provider is a very labor- and capital-intensive business. Provider organizations must have a large number of relatively expensive staff such as physicians, nurses, and other health care professionals. Few other industries have this density of expensive workers. Health care providers, particularly hospitals, must invest large sums of money in buildings, supplies, and equipment. Manufacturers are also capital intensive; they must invest in plants and manufacturing equipment. However, most services organizations, for example, law firms, consulting organizations, and financial institutions do not have the same levels of demand for buildings and equipment.

Hence the relatively low percentages result from the need to make significant investments and bear significant ongoing costs in other aspects of the organization. The salaries of health care professionals and the costs of buildings, supplies, and equipment overshadow health care IT costs.

Other factors also play a role in producing relatively low levels of health care investment in IT:

- For many years health care organizations viewed IT as important for supporting day-to-day operations but not important strategically. An organization might believe that it was strategically more important to establish a new imaging center than it was to invest in an electronic medical record system. To a degree this orientation is changing as health care organizations realize that they cannot accomplish care improvement (and many other) goals without substantial IT investments. However, it can also be argued that IT is less important in health care than other industries. If a bank's computer systems stop working, the bank immediately stops working. No checks can be cashed. Taking deposits becomes difficult. In contrast, if a hospital's systems stop working, surgery can go on, medications can be given, and phlebotomists can draw blood.

- Health care organizations have fewer ways than other types of organizations do to obtain capital. Publicly traded organizations can issue stock. Health care organizations often have small operating margins that make it difficult for them to obtain loans from the bond market. This often-limited ability to obtain capital hinders these organizations' ability to make large IT investments.
- Many health care organizations are very small, having revenues of less than \$100 million. Small organizations face a very difficult time hiring and retaining talented IT staff. This problem can make an organization hesitant to pursue IT investments because it is not sure that it can support the systems.
- IT investments often have their most significant impact when the operations that they are to support are complex and have large volumes of activity. For a small health care organization, the volume and complexity of activity may be sufficiently limited that an IT investment would not result in enough gain to justify that investment.

Structure of the Health Care Market

Table A.2 provides the taxonomy of the health care industry as defined by the North American Industry Classification System (NAICS). The NAICS outlines three major industry segments: payers, providers, and government health care. Each of the sectors in this classification (with each sector having a different NAICS code) represents a different submarket in health care. Some IT companies focus on the federal health care system, others on nursing homes, and yet others on physician offices. Some focus even more narrowly. Within the hospital sector (NAICS code 6222), for example, some IT companies focus on large academic medical centers and others focus on small community hospitals.

The health care IT market is not homogeneous. Different companies serve different segments. Some companies serve multiple segments by carrying diverse product lines or offering systems that will work in multiple sectors—for example, a clinical laboratory system is of interest to civilian and federal hospitals, large physician groups, and freestanding clinical laboratories.

A rough taxonomy of companies that serve health care can be constructed:

- Some companies strive to have a product and service line that covers the full spectrum of health care settings. Hence these companies will offer hospital information systems, physician office systems, nursing home applications, and applications for ancillary departments, such as radiology.
- Several companies focus on a specific setting—for example, hospitals or the physician's office, but not both.
- Some companies offer products that support an application needed by multiple sectors—for example, pharmacy systems or systems that support claims electronic data interchange between providers and payers.

TABLE A.2. HEALTH CARE VERTICAL MARKET: NAICS TAXONOMY.

Health Care Providers	Ambulatory Services	Physician offices Dentist offices Other health Outpatient centers Laboratories Home health
	Hospitals	General medical and surgical Psychiatric and substance abuse Specialty hospitals
	Nursing and residential care	Nursing care Mental care Elderly care
Insurance	Health	Accident and health insurance Hospital and medical Service plans
Government health		Federal hospitals Local hospitals Government psychiatric and long-term care

Source: Cruz, 2003.

- Some companies offer infrastructure—for example, workstations, networks, and servers, which are used by all sectors. These companies usually do not offer applications.
- Several companies offer services used by multiple sectors—for example, IT strategic planning, application implementation, and consulting services.
- Some companies focus their service offerings on a specific type of organization—for example, improving the operations of physician practices—or a specific type of service—for example, improving collections of overdue payments for a provider billing office.

There are literally thousands of companies that support the IT needs of the health care industry. In any given year, hundreds of companies may go out of business and hundreds of new companies may emerge. You can gain an appreciation of the diversity of health care IT companies by attending a large health care IT conference such as the annual conference of the Healthcare Information and Management Systems Society (HIMSS) and visiting the exhibit hall.

Later in this Appendix, we will present sources of IT information. These sources often discuss the products and services of health care IT companies.

Major Suppliers of Health Care IT Products and Services

Table A.3 provides a summary of the top vendors in the industry. These data, collected by the publication *Healthcare Informatics* (Kittleson, 2003), rank companies according to their self-reported health care IT revenue. Use such lists with caution of course. In any given year, some companies will be acquired, and others will experience dramatic upturns and downturns in financial performance. Companies will disappear from the list, and companies will arrive on the list over the course of time. The products and services listed in Table A.3 are illustrative but do not make up a comprehensive list. Several companies that are major infrastructure suppliers—for example, Hewlett

**TABLE A.3. MAJOR HEALTH CARE IT VENDORS:
RANKED BY REVENUE.**

Company	Health Care IT Revenues (2002)	Types of Products and Services
GE Medical Systems Information Technology	\$1.8B	Patient monitoring; diagnostic imaging; clinical information systems
Electronic Data Systems (EDS)	\$1.7B	Health plan applications; system integration; outsourcing; consulting
Phillips Medical Systems	\$1.7B	Patient monitoring; diagnostic imaging
McKesson Information Solutions	\$1.0B	Full range of applications for providers
ACS	\$1.0B	IT and business process outsourcing
Computer Sciences Corp.	\$800M	System integration; outsourcing; consulting
WebMD	\$800M	Insurance EDI; practice management applications; health information
Cerner Corp	\$750M	Full range of applications for providers
Cap Gemini Ernst and Young	\$700M	Consulting; implementation services
Perot Systems	\$600M	System integration; outsourcing; consulting
Ingenix	\$500M	Data analysis services
Medquist	\$500M	Transcription services
IDX Systems Corp	\$460	Full range of applications for providers

Source: Company and revenue data from Kittleson, 2003.

Packard and IBM—either did not report for this survey or do not track health care–specific revenues. Moreover, the fact that a company is large does not mean that it has the best solution for a particular need of a particular organization.

Nonetheless, the data in Table A.3 are interesting for several reasons:

- Health care leadership should know the names and have a reasonable understanding of the major IT vendors that serve their type of organization; sooner or later the organization will be doing business with some of these vendors.
- The size of some of these companies is apparent, with several companies taking in over \$1 billion in revenue.
- The diversity of products and services is also apparent. Some companies focus on applications, whereas others focus on consulting, outsourcing, data analysis, or transcription services.

When an organization needs to turn to the market for applications, infrastructure, or services, its leadership would be well served by reviewing several of the sources of information described in this Appendix, talking to colleagues who may have recently pursued similar IT products and services, and engaging the services of consultants who keep close tabs on the health care IT industry.

Sources of Industry Information

It is essential that the health care professional identifies sources that he or she can trust for current information on health care IT. This textbook cannot examine all the terrain covered by this industry. Moreover, the face of the industry can change quickly. New companies arrive as others disappear. New technologies emerge, and our understanding of current technologies improves. Federal legislation that affects what health care IT is expected to do can surface rapidly.

These sources of information should be diverse: colleagues, consultants, vendors, conferences, and trade press. It takes time and some effort to identify your best sources. You will find some consultants helpful and others not so helpful. You will note that some publications are insightful and others are not.

The following sections provide a brief overview of publications you may find useful.

Periodicals

Among the high-quality health care information technology periodicals (journals and magazines) are

- *Advances for Health Information Executives*
- *Health Data Management*
- *Health-IT World*
- *Health Management Technology*
- *Healthcare Informatics*
- *Healthcare IT News*

All the associations discussed later in this Appendix also publish journals, magazines, or newsletters.

These publications can be supplemented with periodicals that cover the overall IT industry. They include

- *CIO*
- *Computerworld*
- *Information Week*
- *Infoworld*

Several periodicals focus on vertical segments of technology; *Database Management*, *Network World*, and *PC Week* are examples.

Several periodicals address cross-industry management issues, including IT. These publications include

- *Business Week*
- *The Economist*
- *The Harvard Business Review*
- *MIS Quarterly*
- *MIT Sloan Management Review*

In addition, there are magazines and journals that cover health care broadly. They often publish articles and stories on IT issues:

- *Health Affairs*
- *Hospitals and Health Networks*
- *Modern Healthcare*

You can obtain subscription information for these publications by visiting their Web sites. A visit to a university library, medical library, or large public library and an afternoon spent perusing these publications would be worthwhile.

Books

In any given year, several books that cover various aspects of health care IT are published. Publishers that routinely produce such books and publish conference proceedings include

- Aspen Publishers
- Elsevier
- Health Administration Press
- Healthcare Information and Management Systems Society
- Jossey-Bass
- OmniPress
- IOS Press
- Springer-Verlag
- John Wiley & Sons

Industry Research Firms

Finally, there are industry research firms that routinely cover IT generally and health care specifically. Such firms include Forrester, Gartner, HIMSS Analytics, and Meta. These firms, and others, do a nice job of analyzing industry trends, critiquing the products and services of major vendors, and assessing emerging technologies and technology issues. They provide written analyses, conferences, and access to their analysts.

Health Care IT Associations

All health care professionals should join associations that are dedicated to advancing and educating their profession. Health care CFOs often join the Healthcare Financial Management Association, and health care executives routinely join the American College of Healthcare Executives.

These associations serve several useful purposes for the person who joins. They provide

- Publications on topics of interest to the profession
- Conferences, symposiums, and other educational programs
- Information on career opportunities and career development opportunities
- Data that can be used to compare performance across organizations
- Opportunities to meet colleagues who share similar jobs and hence have similar challenges and interests
- Staff who work with legislators and regulators on issues that affect the profession

These association products and services can be invaluable sources of information and experience for any organization or individual.

The health care IT industry has several associations that serve the needs of the health care IT professional. People who are not health care IT professionals will find that their own profession's association also routinely provides periodical articles and conference sessions that cover IT issues. For example, the Healthcare Financial Management Association may present conference sessions on IT advances in analyzing the costs of care or in streamlining patient accounting and billing processes.

The health care IT industry associations are discussed in the following sections. Additional information on these associations can be obtained through the association Web sites.

American Health Information Management Association (AHIMA)

AHIMA is an association of health information management professionals. AHIMA serves largely what has historically been known as the medical records professional. AHIMA's members confront a diverse range of issues associated with both the paper and the electronic medical record, including privacy, data standards and coding, management of the record, appropriate uses of medical record information, and state and federal regulations that govern the medical record.

AHIMA sponsors an annual conference, produces publications, makes a series of knowledge resources available (news, practice guidelines, and competency tests), posts job opportunities, supports distance learning opportunities, and engages in federal and state policy lobbying. AHIMA also offers local and state chapters, which have their own conferences and resources.

The medical records profession has a process for certifying the skill levels of its professionals. AHIMA manages that certification process.

American Medical Informatics Association (AMIA)

AMIA is an association of individuals and organizations "dedicated to developing and using information technologies to improve health care." AMIA focuses on clinical information systems, and a large portion of its membership has interest and training in the academic discipline of medical informatics. AMIA brings together an interesting mixture of practitioners and academics.

AMIA offers an annual symposium, a spring congress, a journal, a series of working groups and special interest groups, and a resource center with job opportunities, publications, and news. AMIA carries out initiatives designed to influence federal policy on health care IT issues.

College of Healthcare Information Management Executives (CHIME)

CHIME is an association dedicated to advancing the health care chief information officer profession and improving the strategic use of IT in health care (CIOs were discussed in Chapter Thirteen). CHIME provides two annual forums, a newsletter, employment information, a data warehouse of information contributed by its members and vendors, distance learning sessions, and classroom-style training. CHIME is partially supported by the CHIME Foundation, established by a nonprofit group of vendors and consultants committed to advancing the CIO profession.

Healthcare Information and Management Systems Society (HIMSS)

HIMSS is an association dedicated to “providing leadership for the optimal use of health care information technology and management systems for the betterment of human health.” HIMSS members are diverse, covering all segments and professions in the health care IT industry.

HIMSS sponsors an annual conference and series of symposiums and smaller conferences. It publishes books, a journal, and newsletters. HIMSS member services include employment information, industry and vendor information, certification programs, distance learning, and white papers. The association has special interest groups and local chapters, and it is actively working with the federal government to develop policy.

HIMSS also has a subsidiary, the Center for Healthcare Information Management (CHIM). CHIM’s membership comprises health care IT vendors and consultants who are committed to advancing the health care IT industry.

Other Industry Groups and Associations

Within the health care IT industry, organizations also exist that serve the needs of health care organizations (in contrast to the individual professional). This section will not attempt to list and describe them. However, examples include the University HealthSystem Consortium, which serves academic health centers; Voluntary Hospitals of America, which provides services to hospitals; and the Scottsdale Institute, whose members are large integrated delivery systems. These and other similar organizations have a partial or dedicated focus on health care IT.

All the associations and groups mentioned in this discussion provide publications and conferences. In addition, companies whose business is putting on conferences sometimes offer health care IT events. Quality publications in addition to those listed previously are available. The reader who is interested in developing a deeper

appreciation of the wealth of conference and publication opportunities can type “healthcare IT publications” and “healthcare IT conferences” into a Web search engine to locate many on-line sources of information.

Summary

The health care IT industry is large and growing. The many pressures on health care organizations to perform and comply are leading them to invest in IT. The industry is served by a multitude of companies that provide products and services. These companies are diverse, both in revenue and in their choice of focus within the submarkets that compose the health care industry.

Professionals in the health care IT industry have formed associations that serve their information and development needs. These associations and industry publications are terrific sources of information on industry issues, emerging technologies, and the strengths and weaknesses of companies serving the industry. The industry faces a core challenge in its application of IT to improve health care; the complexities of care processes, medical data, and health care are often proving to have no boundaries.

Appendix A: Learning Activities

1. Identify two companies that serve the health care IT market. Write a summary that lists each company’s products, services, market focus, and size. Compare the two companies.
2. Pick one of the health care IT associations listed in this Appendix. Develop a summary that describes the association’s membership, activities, products, and services.
3. Select two periodicals that serve the health care IT industry and review an issue of each one. Comment on the types of topics and issues that these publications address.



APPENDIX B

SAMPLE PROJECT CHARTER

Information Systems
Mobile Mammography Van
Project Charter
Version 1.0
Created: 08/01/2003
Printed:
Prepared by: Sam Smith
Presented to: Karen Zimmerman

Project Charter Table of Contents

REVISION HISTORY

FOREWORD

BUSINESS REQUIREMENTS

Background

Project Overview

Project Objectives

Value Provided to Customers

Business Risks

VISION OF THE SOLUTION

Vision Statement

Major Features

Assumptions and Dependencies

Related Projects

SCOPE AND LIMITATIONS

Scope of Initial Release

Scope of Subsequent Releases

Out of Scope

PROJECT SUCCESS FACTORS

BUDGET HIGHLIGHTS

TIMELINE

PROJECT ORGANIZATION

PROJECT MANAGEMENT STRATEGIES

Project Meetings

Issue Management

Scope Change Management

Training Strategy

Documentation Development Strategy

Project Work Paper Organization and Coordination

Revision History

Name	Date	Reason for Changes	Ver./Rev.

Foreword

The purpose of a Project Charter is to document what the Project Team is committed to deliver. It specifies the project timeline, resources, and implementation standards. The Project Charter is the cornerstone of the project, and is used for managing the expectations of all project stakeholders.

A Project Charter represents a formal commitment between Business Sponsors, Steering Committees, the Project Manager, and the Project Team. Therefore it is the professional responsibility of all project members to treat this agreement seriously and make every effort to meet the commitment it represents.

Business Requirements

Background

Sponsored by the Dana Farber Cancer Institute (DFCI) in partnership with the Boston Public Health Commission, neighborhood health centers, and community groups, Boston’s Mammography Van provides mammography screening and breast health education throughout the City of Boston to all women, regardless of ability to pay, with a priority on serving uninsured and underserved women right in their neighborhoods. The Mammography Van began in April of 2002, using IDX for registration, scheduling, and billing. All clinical documentation of the mammography screening has been performed manually since April 2002. Statistical reports generated to maintain state and federal guidelines are all done manually.

Project Overview

The project has two major objectives:

- Implementation of Mammography Patient Manager software to allow for on-line documentation of the clinical encounter with the patient.
- Implementation of a wireless solution on the van at the time of the new software implementation. This will allow for real-time updating of the patient appointment information as well as the ability to register walk-on patients on the spot. On-line documentation will allow ease of reporting to the state and federal agencies.

The products evaluated for implementation are specific to the needs of a mobile program and will meet most, if not all, of the needs of the program.

Project Objectives

Boston's Mobile Mammography Van program will benefit monetarily with a software system because of the reporting capabilities available with on-line documentation. Grant money, as well as state and federal money, is available to the program if evidence is produced to support the needs of the grant and/or the state and federal guidelines of mammography programs. The program will more easily be able to report on the information required by grants and governments to receive funding. There is also the current possibility that we are losing funding based on our current manual reporting practice.

The current program's resources spend valuable time manually calculating statistics. A software system will automate these processes, thus freeing the resources to perform more valuable functions. The van's mammography technician spends a lot of time manually updating and calculating which clients require additional follow-up. A software system will allow real-time reporting of which clients require which type of follow-up. This will decrease the amount of time the technician will spend manually determining which patient requires which follow-up letter. The program will be secure in its adherence to state and federal reporting guidelines for the van program as well as for the technicians working in the program.

Value Provided to Customers

- Improved productivity and reduced rework
- Streamlined business processes
- Automation of previously manual tasks
- Ability to perform entirely new tasks or functions

- Conformance to current standards or regulations
- Improved access to patient clinical and demographic information via remote access
- Reduced frustration level compared to current process

Business Risks

The major risk associated with the implementation is the selection of an incompatible vendor. There is always the concern that with a program that is new to the institution, the understanding needed to fully anticipate the needs of the program is incomplete. In addition, there is the risk that the software solution will increase workload as it offers more functions than are currently available to the user in a manual system.

Risk mitigation action items include this Charter, which should clearly state the “in scope” objectives of the implementation. This should address both risks identified here.

Vision of the Solution

Vision Statement

The Mobile Mammography Van program will be a more efficient and safe environment. The current lack of software system introduces risks due to potential regulatory issues, patient safety issues due to potential missed follow-up, as well as program risks due to potential loss of funding. The proposed implementation of a software system alleviates these risks as well as introduces the prospect of future expansion of the program that is not easily achieved in the current environment.

The program should be able to handle more patients with the new software. The registration and scheduling process will stay the same, but the introduction of remote access will increase efficiency. Changes to appointments or patient demographic data can now occur on the van. An interface with the IDX scheduling and registration software to the mobile mammography software will ensure no duplicate entry of patient data. The ability to document patient history on-line on the van will decrease the amount of paperwork filled out at the end of the day by the technician. There is also the opportunity to better track patients by entering data during the day versus at the end of the day.

The current transcription process is not expected to change. Films will still be read in the current manner, but reports will be saved to a common database. This will allow the technician or program staff to access the reports on-line. Entry of the BIRAD result (mammography result) will occur much more quickly and efficiently. Patient

follow-up based on the BIRAD will be done more quickly as well. Letters can be automatically generated based on the results and printed in batches. All patient follow-up, including phone calls, letters, and certified letters are captured in the system with a complete audit trail. This ensures the program's compliance with regulations concerning patient follow-up.

The film tracking functions will also allow more accurate tracking of the patient's films. Accurate film tracking will increase the turnaround time for film comparisons and patient follow-up.

The ability to customize the software will increase the grant funding possibilities for the program. The program can introduce new variables or queries to the clients in order to produce statistical reports based on the gathered information. Increases in funding can lead to increases in the program's expansion. The increased expansion will increase the availability of free mammography to underprivileged women.

Major Features

- Interface can be implemented from IDX to OmniCare system (OmniCare supports clinical documentation) for registration information.
- Mammography history questionnaires can be preprinted and brought on the van for the patient to fill out.
- OmniCare will allow entry of BIRAD results.
- Transcribed reports can be uploaded or cut and pasted into OmniCare from the common database.
- Patient letters are generated from and maintained in OmniCare.
- Follow-up including pathology results will be maintained in OmniCare.
- Communication management functions will be maintained with full audit trail.
- Film tracking will be done in OmniCare.
- Statistical reporting will be facilitated.

Assumptions and Dependencies

The assumptions and dependencies for this project are few, but all are crucial to the success of the implementation. The software and hardware to be purchased for this implementation are key aspects of the project. The project is dependent on the remote access satellite hardware working as expected. The software vendor chosen during the vendor selection project is assumed to be the best fit for this program. The IDX interface is a crucial assumption in this project. This working interface is key to the efficiencies this program is looking to achieve with the implementation. Resources are an assumption inherent in the budget. Appropriate resources to effectively implement the solution are important to the success of the implementation.

Related Projects

There are no related projects for this project. All needed work is included in this implementation project.

Scope and Limitations

Scope of Initial Release

- IDX interface for patient demographic and registration information
- Film tracking (possible bar coding for film tracking)
- Mammography history questionnaires
- BIRAD result entry
- Patient follow-up management
- Communications management
- Statistical reporting
- Custom fields management
- Remote access satellite installation

Interface Scope

- IDX registration data

Organizational Scope

- The OmniCare implementation will focus on the implementation of the software with the DFCI (Dana Farber Cancer Institute) program of the Boston Mobile Mammography Van. No other partner institutions are involved for roll out. The film reads done at Faulkner Hospital are not included in this scope.

Conversion Scope

- There is no data conversion planned for this project.

Scope of Subsequent Releases

- Future releases may try to include the Faulkner Hospital Radiologists. Currently as Faulkner reads the film, the radiologist dictates and the text is transcribed. It would be more efficient in the future if the radiologists were automatically part of OmniCare.

Out of Scope

- Billing functions are not within the scope of this implementation. Billing is currently done via IDX and will continue this way.
- A results interface is not within the scope of this implementation. The results of the mammograms will be available only on paper in the medical record or within the OmniCare solution. There will be no integration with the Results application.
- Scheduling and registration functions are not in scope for this implementation. These functions are currently done via IDX. An interface from IDX to provide this information in the OmniCare solution is planned.
- Radiologists' entry of data is not in scope for this implementation. It is listed as a possible scope of subsequent releases.

Project Success Factors

- Increased turnaround time for patient follow-up
- Decreased turnaround time with films by film tracking
- Decreased time creating and managing reports
- Increased numbers of mammographies taken
- Decreased time spent by staff on administrative tasks

Budget Highlights

Capital budget	\$52,550
Hardware	\$10,000
Software	\$30,000
Remote access	\$6,200
1st yr. remote svc.	\$1,350
Contingency	\$5,000

Project Staff Resources

IS analyst = .50 FTE for the 6 months

Network services = .25 for the 3–6 months

Karen = 8 hr./wk. for 4 months

Program asst.—Sarah = 12 hr./wk. for 4 months

New person to be hired

Temp to do data entry conversion

Timeline

Project will commence on November 1, 2003, and be completed July 1, 2004.

Approximate date of completion of major phases:

Analysis	January 1, 2004
Satellite installation	February 1, 2004
Registration interface	March 1, 2004
Film tracking	March 1, 2004
History questionnaires	May 1, 2004
Result entry	June 1, 2004
Communications mgmt	June 1, 2004
Patient follow-up	June 1, 2004
Reporting	June 15, 2004

Project Organization

Business Sponsor(s)

Anne Jones, VP of External Affairs

Business Owner(s)

Karen Ruderman, Program Director Boston's Mammography Van

Steering Committee

Karen Zimmerman, Program Director Boston's Mammography Van

Anne Johnson, Director of Planning

Jerry Melini, Technical Director of Radiology

Project Manager

Charles Leoman

Project Team

IS Analysts TBD

Network Services IS staff TBD

Karen Zimmerman, Program Director Boston's Mammography Van
 Sarah Smithson, Program Assistant Boston's Mammography Van
 Data Entry temporary staff

Project Management Strategies

Project Meetings

In order to maintain effective communication with Project Team members and the Mobile Mammography Van community, a series of standing meetings will be conducted. Meeting minutes will be documented and stored on the shared core team directory. The following meetings and facilitated sessions will be held:

Decision-making level	Steering Committee	Project Team
Role	• Resolves show-stopper issues and changes in scope. • Acts as a sounding board for decisions and actions that affect user acceptance of the project. This includes anything that affects project milestones and outcomes. • Reviews decisions, recommendations, and requests that are high in integration and complexity and that are not resolved at the Project Team level. • Scope management and planning.	• Governs the actual work and the progress of the project. • Reviews Project work and status Resource issues Vendor issues Project risks • Serves as working or focus group to report daily progress. • Responsible for implementation decisions that have integration impact and that are of medium or high complexity.
Participants	• Chaired by Business Sponsor. • Key stakeholders on business and IS sides.	• Cochaired by IS Project Manager and Business Owner. • All resources assigned to the project.
Meeting frequency	• Meets regularly to ensure steady project progress.	• Meets, as needed, weekly to monthly, for project status and updates.

Issue Management

Issue identification, management, and resolution are important project management activities. The Project Manager is responsible for the issue management process and works with the Project Team and Steering Committee (if needed) to agree on the resolution of issues.

Effective issue management enables

- A visible decision-making process
- A means for resolving questions concerning the project
- A project issue audit trail

The standard IS project issue management process and forms will be used and attached to the Charter as needed.

Scope Change Management

Scope change management is essential to ensure that the project is managed to the original scope, as defined in this Charter. The purpose of a scope management process is to constructively manage the pressure to expand scope.

Scope expansion is acceptable as long as

- Users agree that the new requirements are justified.
- Impact to the project is analyzed and understood.
- Resulting changes to project (cost, timing, resources, quality) are approved and properly implemented.

Any member of the Project Team or other members of the Mobile Mammography Van community may propose a change to the scope of the project. The requester will initiate the process by completing a Change Request Definition Form. When necessary, the Project Manager will review and seek advice from the Steering Committee on scope changes that affect the project schedule or budget, or both.

The standard IS project scope management process and forms will be used and attached as appendixes to the Charter, as needed.

Training Strategy

Training Scope

The program consists of a program administrator, one mammography technician, one assistant to the administrator, and one patient educator and administration person. All of the employees will be included in training for their specific role related to the process.

The program administrator will learn all of the roles in order to fill in when needed. Additional training will be given to the other employees for backup purposes.

Training Approach

The vendor will provide the training during the initial implementation. The employees of the program will train new employees.

Training Material Development

The vendor will provide training materials.

Documentation Development Strategy

The team will develop the following documentation:

- Technical operations procedure manual
- Policies and procedures related to the use and management of the system
- Application manuals, if needed
- OmniCare technical and application maintenance and support manuals, if needed

Project Work Paper Organization and Coordination

In order to keep the project documentation, meeting minutes, and deliverables organized and accessible to the core team, a project folder on the shared network will be established and maintained.



REFERENCES

- Aarts, J., Doorewaard, H., & Berg, M. (2004). Understanding implementation: The case of a computerized physician order entry system in a large Dutch university medical center. *Journal of the American Medical Informatics Association*, 11(3), 207–216.
- Accreditation Association for Ambulatory Health Care. (2003). *About AAAHC*. Retrieved June 1, 2004, from <http://www.aaahc.org/about/about2.shtml>
- Accredited Standards Committee X12. (2004). *X12N/TG2: Healthcare purpose and scope*. Retrieved July 20, 2004, from http://www.x12.org/x12org/subcommittees/sc_home.cfm?CFID=2056151&CFTOKEN=1
- Agarwal, R., & Sambamurthy, V. (2002). *Organizing the IT function for business innovation leadership*. Chicago: Society for Information Management.
- Agency for Healthcare Research and Quality. (2001). *Reducing and preventing adverse drug events to decrease hospital costs*. Retrieved May 26, 2004, from <http://www.ahrq.gov/qual/aderia/aderia.htm>
- Agency for Healthcare Research and Quality. (2002). *Computerized physician order entry (CPOE) with clinical decision support systems (CDSSs)*. Retrieved December 17, 2003, from <http://www.medrecinst.com/publications/hit/2002/february03.asp>
- Altis, Inc. (2004). *Engines defined*. Retrieved November 2004 from <http://www.altisinc.com/IE/defined.html>
- Amatayakul, M., et al. (2001). *Definition of the health record for legal purposes* (AHIMA Practice Brief). Retrieved December 2004 from http://library.ahima.org/xpedio/groups/publics/documents/ahima/pub_bok1_009223.html
- American Health Information Management Association. (2002a). *Destruction of patient health information (updated)* (Practice Brief). Retrieved November 2004 from http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_016468.html

- American Health Information Management Association. (2002b). *Retention of health information* (Practice Brief). Retrieved June 1, 2004, from http://library.ahima.org/xpedio/groups/publics/documents/ahima/pub_bok1_012545.html
- American Health Information Management Association. (2003a). *Final rule for HIPAA security standards*. Chicago: Author.
- American Health Information Management Association. (2003b). *Implementing electronic signatures* (Practice Brief). Retrieved June 1, 2004, from http://library.ahima.org/intradoc-cgi/idc_cgi_isapi.dll?IdcService=GET_HIGHLIGHT_INF
- American Health Information Management Association. (2004). *A HIPAA security overview* (Practice Brief). Retrieved April 14, 2004, from http://library.ahima.org/intradoc-cgi/idc_cgi_isapi.dll?IdcService=GET_HIGHLIGHT_INF
- American Health Information Management Association, Data Quality Management Task Force. (1998a). *A checklist to assess data quality management effort* (Practice Brief). Retrieved January 8, 2004, from http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_000069.html
- American Health Information Management Association, Data Quality Management Task Force. (1998b). *Data quality management model* (Practice Brief). Retrieved January 8, 2004, from http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_000066.html
- American Medical Association (2005). *CPT-5*. Retrieved February 2005 from <http://www.ama-assn.org/ama/pub/category/3883.html>
- American Medical Association. (2003). *Guidelines for physician-patient electronic communications*. Retrieved November 2004 from <http://www.ama-assn.org/ama/pub/category/print/2386.html>
- American National Standards Institute. (2004). *Standards activities overview*. Retrieved July 19, 2004, from http://www.ansi.org/standards_activities/overview/overview.aspx?menuid=3
- American Osteopathic Association. (2004). *Healthcare facilities*. Retrieved June 1, 2004, from http://do-online.osteotech.org/index.cfm?PageID=acc_hfmain
- American Telemedicine Association. (2003). *Report on reimbursement*. Washington, DC: Author.
- Applegate, L., Austin, R., & McFarlan, W. (2003). *Corporate information strategy and management* (6th ed.). Boston: McGraw-Hill.
- Arlotto, P., & Oakes, J. (2003). *Return on investment: Maximizing the value of healthcare information technology*. Chicago: Healthcare Information and Management Systems Society.
- Arts, D., DeKeizer, N., & Scheffer, G. (2002). Defining and improving data quality in medical registries: A literature review, case study, and generic framework. *Journal of the American Medical Informatics Association*, 9(6), 600–611.
- Ash, J., Gorman, P., Lavelle, M., Lyman, J., & Fournier, L. (2001). Investigating physician order entry in the field: Lessons learned in a multi-center study. *Medinfo*, 10(Part 2), 1107–1111.
- Ash, J., Stavri, P., Dykstra, R., & Fournier, L. (2003). Implementing computerized physician order entry: The importance of special people. *International Journal of Medical Informatics*, 69(2–3), 235–250.
- Associated Press. (1995a, February 28). *7 get fake HIV-positive calls*. Retrieved December 2004 from <http://www.aegis.com/news/ap/1995/AP950248.html>
- Associated Press. (1995b, February 28). *Teen arrested over AIDS call*. Retrieved December 2004 from <http://www.aegis.com/news/ap/1995/AP950249.html>
- Baker, L., Wagner, T. H., Singer, S., & Bundorf, M. K. (2003). Use of the Internet and e-mail for health care information: Results from a national survey. *Journal of the American Medical Association*, 289, 2400–2406.

- Balas, D., Weingarten, S., Garb, C., Blumenthal, D., Boren, S., & Brown, G. (2000). Improving preventive care by prompting physicians. *Archives of Internal Medicine*, 160(3), 301–308.
- Barlas, S. (2002, September). Report from the FDA's bar coding initiative. *Healthcare Informatics*, pp. 17–18.
- Barlow, S., Johnson, J., & Steck, J. (2004). The economic effect of implementing an EMR in an outpatient clinical setting. *Journal of Healthcare Information Management*, 18(1), 46–51.
- Bates, D., & Gawande, A. (2003). Improving safety with information technology. *New England Journal of Medicine*, 348, 2526–2534.
- Bates, D., Kuperman, G., Rittenberg, J., Teich, J., Fiskio, J., Ma'luf, N., et al. (1999). A randomized trial of a computer-based intervention to reduce utilization of redundant laboratory tests. *American Journal of Medicine*, 106(2), 144–150.
- Bates, D., Kuperman, G., & Teich, J. (1994). Computerized physician order entry and the quality of care. *Quality Management in Health Care*, 2, 18–27.
- Bates, D., Leape, L., Cullen, D., Laird, N., Peterson, L., Teich, J., et al. (1998). Effect of computerized physician order entry and a team intervention on prevention of serious medication errors. *Journal of the American Medical Association*, 280, 1311–1316.
- Bates, D., Miller, E., Cullen, D., Burdick, L., Williams, L., Laird, N., et al. (1999, November 22). Patient risk factors for adverse drug events in hospitalized patients. *Archives of Internal Medicine*, 159, 2553–2560.
- Bates, D., Teich, J., Lee, J., Seger, D., Kuperman, G., Ma'luf, N., et al. (1999). The impact of computerized physician order entry on medication error prevention. *Journal of the American Medical Informatics Association*, 6(4), 313–321.
- Bazzoli, F. (2004, May). NAHIT IT standards directory aims to provide common ground. *Healthcare IT News*, p. 5.
- Bensaou, M., & Earl, M. (1998). The right mind-set for managing information technology. *Harvard Business Review*, 76(5), 119–128.
- Berg, M. (2001). Implementing information systems in health care organizations: Myths and challenges. *International Journal of Medical Informatics*, 64(2–3), 143–156.
- Berkman, E. (2002, February 1). How to stay ahead of the curve. *CIO*. Retrieved December 2004 from <http://www.cio.com/archive/020102/enterprise.html>
- Berman, J., Zaran, F., & Rybak, M. (1992). Pharmacy-based antimicrobial-monitoring service. *American Journal of Hospital Pharmacy*, 49, 1701–1706.
- Bleich, H., Safran, C., & Slack, W. (1989). Departmental and laboratory computing in two hospitals. *M.D. Computing*, 6(3), 149–155.
- Brailer, D., & Terasawa, E. (2003). *Use and adoption of computer-based patient records*. Oakland, CA: California HealthCare Foundation.
- Bresnahan, J. (1998, July 15). What good is technology? *CIO Enterprise*, pp. 25–26, 28, 30.
- Briney, A. (2000). *2000 Information Security industry survey*. Retrieved November 2004 from <http://www.infosecuritymag.com>
- Briney, A. (2001). *2001 Information Security industry survey*. Retrieved November 2004 from <http://www.infosecuritymag.com>
- Brown, C., & Sambamurthy, V. (1999). *Repositioning the IT organization to enable business transformation*. Chicago: Society for Information Management.
- Brown, J., & Hagel, J. (2003). Does IT matter? *Harvard Business Review*, 81, 109–112.
- Brown, N. (2002). *Telemedicine Research Center: What is telemedicine?* Retrieved Oct 14, 2003, from <http://trc.telemed.org/telemedicine/primer.asp>
- Brown, N. (2004). *Telemedicine 101: Understanding telemedicine*. Retrieved November 2004 from <http://tie.telemed.org>

- Burke, J., & Pestotnik, S. (1999). Antibiotic use and microbial resistance in intensive care units: Impact of computer-assisted decision support. *Journal of Chemotherapy*, 11, 530–535.
- Burnum, J. (1989). The misinformation era: The fall of the medical record. *Annals of Internal Medicine*, 110, 482–484.
- California HealthCare Foundation. (1999). *Medical Privacy and Confidentiality Survey summary and overview*. Retrieved December 2004 from <http://www.chcf.org/documents/ihealth/survey.pdf>
- Carr, N. (2003). IT doesn't matter. *Harvard Business Review*, 81, 41–49.
- Cash, J., McFarlan, W., & McKenney, J. (1992). *Corporate information systems management: The issues facing senior executives*. Chicago: Irwin.
- Cecil, J., & Goldstein, M. (1990). Sustaining competitive advantage from IT. *McKinsey Quarterly*, 4, 74–89.
- Centers for Medicare and Medicaid Services. (2002a). *The CMS Chart Series*. Retrieved from <http://www.cms.hhs.gov/charts/series>
- Centers for Medicare and Medicaid Services (2002b). *Standards for Privacy of Individually Identifiable Health Information: Final Rule*. Retrieved February 2005 from <http://www.hhs.gov/ocr/hippa/prirulepd.pdf>
- Centers for Medicare and Medicaid Services. (2004). *HIPAA administrative simplification: Security: Final rule*. Retrieved November 2004 from <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security>
- Chin, T. (2003). *Doctors pull plug on paperless systems*. Retrieved February 17, 2003, from <http://www.ama-assn.org/amednews/2003/02/17/bil20217.htm>
- Christensen, C. (1997). *The innovator's dilemma*. Boston: Harvard Business School Press.
- Christensen, C. (2001). The past and future of competitive advantage. *MIT Sloan Management Review*, 42(2), 105–109.
- College of Healthcare Information Management Executives. (1998). *The healthcare CIO: A decade of growth*. Ann Arbor, MI: Author.
- Collins, J. (2001). *Good to great*. New York: HarperCollins.
- Commission on Accreditation of Rehabilitation Facilities. (2004). *What does CARF accredit?* Retrieved June 1, 2004, from <http://www.carf.org/consumer.aspx?Content=Content/ConsumerServices/cs05en.html&ID=5>
- Committee on Workforce Needs in Information Technology. (2001). *Building a workforce for the information economy*. Washington, DC: National Academies Press.
- Committee to Study the Impact of Information Technology on the Performance of Service Activities. (1994). *Information technology in the service society*. Washington, DC: National Academies Press.
- Common Criteria. (2004). *Common criteria for information technology security evaluation* (No. CCIMB-2004-01-001). Retrieved November 2004 from www.commoncriteriaportal.org
- Computer Sciences Corporation. (2001). *Critical issues of information systems management*. El Segundo, CA: Computer Sciences Corporation.
- Connecticut health plan to expand online physician consultation program. (2002, November 18). *iHealthBeat* (California HealthCare Foundation). Retrieved December 2004 from <http://www.ihealthbeat.org/index.cfm?action=lookupID&id=23988>
- Cruz, G. (2003). *In unforgiving times, the US healthcare market boosts IT spending, 2001–2006* (ID No. ITGI-WW-MS-0125). Stamford, CT: Gartner, Inc.
- Davenport, T., & Short, J. (1990, Summer). The new industrial engineering: Information technology and business process redesign. *MIT Sloan Management Review*, pp. 11–27.
- DeLuca, J., & Enmark, R. (2002). *The CEO's guide to health care information systems* (2nd ed.). San Francisco: Jossey-Bass.

- Department of Defense. (1985). *Trusted computer system evaluation criteria* (DOD 5200.28-STD). Retrieved November 2004 from <http://www.radium.ncsc.mil/tpcp/library/rainbow/5200.28-STD.html>
- Department of Health and Human Services. (2002). *Health insurance reform: Modifications to electronic data transaction standards and code sets* (No. CMS-0003/5-F). Bethesda, MD: Author.
- Department of Health and Human Services. (2004.) *The National Healthcare Information Infrastructure: FAQ sheet*. Retrieved November 2004 from <http://aspe.hhs.gov/sp/nhii>
- Department of Health and Human Services, Office of Inspector General. (2004). *Fraud prevention and detection. Compliance guidance*. Retrieved November 2004 from www.oig.hhs.gov
- Department of Labor, Bureau of Labor Statistics (2004). *Occupational outlook handbook*. Retrieved November 2004 from <http://www.bls.gov/oco/ocos110.htm>.
- Donald, J. (1989). Prescribing costs when computers are used to issue all prescriptions. *British Medical Journal*, 299, 28–30.
- Dougherty, M. (2001). On the line: Professional practice solutions. *Journal of AHIMA*, 72(10), 72–73.
- Downes, L., & Mui, C. (1998). *Unleashing the killer app*. Boston: Harvard Business School Press.
- Dragoon, A. (2003, August 15). Deciding factors. *CIO*, pp. 49–59.
- Drazen, E., & Straisor, D. (1995). *Information support in an integrated delivery system*. Paper presented at the 1995 annual HIMSS conference, Chicago.
- Duxbury, B. (1982). Therapeutic control of anticoagulant treatment. *British Medical Journal*, 284, 702.
- Dvorak, R., Holen, E., Mark, D., & Meehan, W., III (1997). Six principles of high-performance IT. *McKinsey Quarterly*, 3, 164–177.
- Earl, M. (1993). Experiences in strategic information systems planning. *MIS Quarterly*, 17(1), 1–24.
- Earl, M., & Feeney, D. (1995). Is your CIO adding value? *McKinsey Quarterly*, 2, 144–161.
- Earl, M., & Feeney, D. (2000). How to be a CEO for the information age. *MIT Sloan Management Review*, 41(2), 11–23.
- eHealth Initiative. (2004). Retrieved December 2004 from http://www.ehealthinitiative.org/december_6_meeting.msp
- EHR Collaborative. (2004). *Who we are*. Retrieved November 2004 from www.ehrcollaborative.org
- Eng, J. (2001). Computer network security for the radiology enterprise. *Radiology*, 220(2), 304–309.
- Etheridge, Y. (2001, January). PKI: How and why it works. *Health Management Technology*, pp. 20–21.
- Evans, J., & Hayashi, A. (1994, September–October). Implementing on-line medical records. *Document Management*, pp. 12–17.
- Evans, R., Pestotnik, S., Classen, D., Bass, S., & Burke, J. (1992). *Prevention of adverse drug events through computerized surveillance*. Paper presented at the Annual Symposium on Computer Applications in Medical Care.
- Evans, R., Pestotnik, S., Classen, D., & Burke, J. (1993). Development of an automated antibiotic consultant. *M.D. Computing*, 10(1), 17–22.
- Evans, R. S., Pestotnik, S., Classen, D., Clemmer, T., Weaver, L., Orme, J. F., et al. (1998). A computer-assisted management program for antibiotics and other antiinfective agents. *New England Journal of Medicine*, 228, 232–238.
- Feld, C., & Stoddard, D. (2004). Getting IT right. *Harvard Business Review*, 82(2), 72–79.
- First Consulting Group. (2003, January). *Computerized physician order entry: Costs, benefits, and challenges: A case study approach*. New York: Author.
- Fluke Networks. (2003). *Wireless security notes: A brief analysis of risks*. Retrieved December 2004 from http://wp.bitpipe.com/resource/org_1014144860_961/fnet_wireless_security_bpx.pdf

- Framework Definition/Architecture Quickstart*. (2004). Retrieved July 19, 2004, from <http://www.zifa.com/quickstart.html>
- Freedman, D. (1991, July). The myth of strategic I.S. *CIO*, pp. 34–41.
- Gadd, C., & Penrod, L. (2000). Dichotomy between physicians' and patients' attitudes regarding EMR use during outpatient encounters. *Proceedings of the American Medical Informatics Association Symposium*, pp. 275–279.
- Garrett, L., Jr., Hammond, W., & Stead, W. (1986). The effects of computerized medical records on provider efficiency and quality of care. *Methods of Information in Medicine*, 25(3), 151–157.
- Glaser, J. (1991, January–February). Managing the management of information systems. *Healthcare Executive*, pp. 34–38.
- Glaser, J. (2002). *The strategic application of information technology in health care organizations* (2nd ed.). San Francisco: Jossey-Bass.
- Glaser, J. (2003a, March). Analyzing information technology value. *Healthcare Financial Management*, pp. 98–104.
- Glaser, J. (2003b, September). When IT excellence goes the distance. *Healthcare Financial Management*, pp. 102–106.
- Glaser, J., DeBor, G., & Stuntz, L. (2003). The New England Healthcare EDI network. *Journal of Healthcare Information Management*, 17(4), 42–50.
- Goldsmith, J. (2003). *Digital medicine implications for healthcare leaders*. Chicago: Health Administration Press.
- Gopalakrishna, R. (2000). *Audit trails*. Retrieved July 21, 2004, from <http://www.cerias.purdue.edu/homes/rgk/at.html>
- Gue, D. (2003). *The HIPAA Security Rule (NPRM): Overview*. Retrieved April 13, 2004, from <http://www.hipaadvisory.com/regs/securityoverview.htm>
- Haddad, S., Potvin, L., Roberge, D., Pineault, R., & Remondin, M. (2000). Patient perception of quality following a visit to a doctor in a primary care unit. *Family Practice*, 17(1), 21–29.
- Hammer, M., & Champy, J. (1993). *Reengineering the corporation: A manifesto for business revolution*. New York: HarperCollins.
- Hammond, W., & Cimino, J. (2001). Standards in medical informatics. In E. Shortliffe & L. Perreault (Eds.), *Medical informatics computer applications in health care and biomedicine* (pp. 212–256). New York: Springer-Verlag.
- Hankin, R. (2002). *Bar coding in healthcare: A critical solution*. Retrieved July 19, 2004, from <http://www.bbriefings.com/cdps/cditem.cfm?NID=753&CID=5&CFID=250074&CFTO>
- Hatoum, H., Catizone, C., Hutchinson, R., & Purohit, A. (1986). An eleven-year review of the pharmacy literature: Documentation of the value and acceptance of clinical pharmacy. *Drug Intelligence & Clinical Pharmacy*, 20, 33–48.
- Health Level Seven Canada. (2004). *The components of an HL7 message*. Retrieved November 2004 from <http://www.interfaceware.com/manual/ch-2-1-3.html>
- Health Privacy Project. (1999). *Exposed: A health privacy primer for consumers*. Retrieved December 2004 from http://www.healthprivacy.org/usr_doc/34775.pdf
- Health Privacy Project. (2003). *Health privacy 101: Medical privacy stories*. Retrieved November 2004 from www.healthprivacy.org
- Healthcare Information and Management Systems Society. (2003a). *15th Annual HIMSS Leadership Survey sponsored by Superior Consultant Company*. Retrieved November 2004 from http://www.himss.org/2004survey/ASP/healthcarecio_home.asp
- Healthcare Information and Management Systems Society. (2003b). *Implementation guide for the use of bar code technology in healthcare*. Chicago: Author.

- Healthcare Information and Management Systems Society. (2004). *Awards*. Retrieved November 2004 from <http://www.himss.org/ASP/awards.asp>
- HealthGrades. (2004). *Hospital report cards*. Retrieved July, 20, 2004, from <http://www.healthgrades.com/public/index.cfm?fuseaction=mod&modtype=HRC&modact>
- Henderson, J., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 32(1), 4–16.
- Hershey, C., McAloon, M., & Bertram, D. (1989). The new medical practice environment: Internists' view of the future. *Archives of Internal Medicine*, 149, 1745–1749.
- Herzlinger, R. (1997). *Market-driven health care*. Reading, MA: Addison-Wesley.
- Hughes, G. (2000). Portable computer security (AHIMA Practice Brief). *Journal of the American Health Information Association*, pp. 80A–80B.
- Institute of Medicine. (1991). *The computer-based patient record: An essential technology for health care*. Washington, DC: National Academies Press.
- Institute of Medicine. (2000). *To err is human: Building a safer health system*. Washington, DC: National Academies Press.
- Institute of Medicine. (2001). *Crossing the quality chasm: A new health system for the 21st century*. Washington, DC: National Academies Press.
- Institute of Medicine, Committee on Data Standards for Patient Safety. (2003a). *Key capabilities of an electronic health record system*. Washington, DC: Author.
- Institute of Medicine, Committee on Data Standards for Patient Safety. (2003b). *Reducing medical errors requires national computerized information systems: Data standards are crucial to improving patient safety*. Retrieved November 20, 2003, from <http://www4.nationalacademies.org>
- Institute of Medicine, Committee on Data Standards for Patient Safety. (2004). *Patient safety: Achieving a new standard for care*. Washington, DC: National Academies Press.
- Jenkins, M., & Bond, C. (1996). The impact of clinical pharmacists on psychiatric patients. *Pharmacotherapy*, 16, 708–714.
- Johns, M. (1997). *Information management for health professionals*. Albany, NY: Delmar.
- Johnston, B., Wheeler, L., Deuser, J., & Sousa, K. (2000). Outcomes of the Kaiser Permanente Tele-Home Health research project. *Archives of Family Medicine*, 9(1), 40–45.
- Johnston, D., Pan, E., Walker, J., Bates, D., & Middleton, B. (2003). *The value of computerized provider order entry in ambulatory settings*. Chicago: Healthcare Information and Management Systems Society.
- Johnston, D., Pan, E., Walker, J., Bates, D., & Middleton, B. (2004). *Patient safety in the physician's office: Assessing the value of ambulatory CPOE*. Oakland, CA: California HealthCare Foundation.
- Joint Commission on Accreditation of Healthcare Organizations. (2004a). *JCAHO hospital accreditation manual 2004*. Oakbrook Terrace, IL: Author.
- Joint Commission on Accreditation of Healthcare Organizations. (2004b). *Specification manual for national implementation of hospital core measures: Version 2.0: Implementation to begin with July 2004 discharges*. Retrieved July 20, 2004, from <http://www.jcaho.org/pms/core+measures/information+on+final+specifications.htm>
- Joint Commission on Accreditation of Healthcare Organizations. (2004c). *What is the Joint Commission on Accreditation of Healthcare Organizations?* Retrieved June 1, 2004, from <http://www.jcaho.org/general+public/who+jc/index.htm>
- Karson, A., Kuperman, G., Horsky, J., Fairchild, D., Fiskio, J., & Bates, D. (1999, April). Patient-specific computerized outpatient reminders to improve physician compliance with clinical guidelines. *Journal of General Internal Medicine*, 14(Suppl. 2), 126.

- Kaushal, R., & Bates, D. (2002). Information technology and medication safety: What is the benefit? *Quality Safe Health Care*, 11, 261–265.
- Keen, P. (1997). *The process edge*. Boston: Harvard Business School Press.
- Kelly, D. (2003). *Applying quality management in healthcare: A process improvement*. Chicago: Health Administration Press.
- Kelly, P., & Legrow, G. (2000). *Medicaid health plans: Are application service providers right for you? A market segment report*. Oakland, CA: California Healthcare Foundation.
- Kennedy, O., Davis, G., & Heda, S. (1992). Clinical information systems: 25-year history and the future. *Journal of the Society for Health Systems*, 3(4), 49–60.
- Kilbridge, P., et al. (1998). Information systems for IDNs: Best practices and key success factors. In *Proceedings of the 1998 annual HIMSS conference* (pp. 229–241). Chicago: Healthcare Information and Management Systems Society.
- Kittleson, B. (2003, June). The Healthcare Informatics 100. *Healthcare Informatics*, pp. 33–63.
- Kuperman, G., Teich, J., Gandhi, T., & Bates, D. (2001). Patient safety and computerized medication ordering at Brigham and Women's Hospital. *Joint Commission Journal on Quality Improvement*, 27(10), 509–521.
- Kurtz, M. (2002). HL7 Version 3.0: A preview for CIOs, managers, and programmers. *Journal of Healthcare Information Management*, 16(4), 22–23.
- Lake, K. (1998). Cashing in on your ATM network. *McKinsey Quarterly*, 1, 173–178.
- Landis, S., Hulkower, S., & Pierson, S. (1992). Enhancing adherence with mammography through patient letters and physician prompts: A pilot study. *North Carolina Medical Journal*, 53(11), 575–578.
- Langberg, M. L. (2004). *Challenges to implementing CPOE: A case study of a work in progress at Cedars-Sinai*. Retrieved April 2004 from <http://www.modernphysician.com/page.cms?pageId=216>
- LaTour, K. (2002). Healthcare information standards. In K. LaTour & S. Eichenwald (Eds.), *Health information management concepts, principles, and practice* (pp. 121–136). Chicago: American Health Information Management Association.
- Leapfrog Group. (2002). 70% percent of all Americans can now get Leapfrog patient safety information for hospitals in their area. Retrieved December 29, 2004, from http://www.leapfroggroup.org/media/file/Leapfrog-New_Region_Data_Release_11-14-02.pdf.
- Leapfrog Group. (2004a). *The Leapfrog safety practices*. Retrieved November 2004 from http://www.leapfroggroup.org/for_hospitals/leapfrog_safety_practices
- Leapfrog Group. (2004b). *Rewarding higher standards*. Retrieved July 20, 2004, from <http://www.leapfroggroup.org>
- Lee, F. W. (2002). Data and information management. In K. LaTour & S. Eichenwald (Eds.), *Health information management concepts, principles, and practice* (pp. 83–100). Chicago: American Health Information Management Association.
- Lee, F. W. (in press). Establishing a health record security program. In *Privacy and security in health information management: Principles and practice*. Chicago: American Health Information Management Association.
- Legler, J., & Oates, R. (1993). Patients' reactions to physician use of a computerized medical record system during clinical encounters. *Journal of Family Practice*, 37(3), 241–244.
- Lesar, T., Briceland, L., & Stein, D. (1997). Factors related to errors in medication prescribing. *Journal of the American Medical Association*, 277, 312–317.
- Levinson, M. (2001, February 1). *Jackpot*. Retrieved November 2004 from http://www.cio.com/archive/020103/tl_profile.html

- Levit, K., Cowan, C., Lazenby, H., Sensenig, A., McDonnell, P., Stiller, J., et al. (2000). Health spending in 1998: Signals of change. *Health Affairs*, 19(1), 124–132.
- Libicki, M., Schneider, J., Frelinger, D., & Slomovic, A. (2000). *Scaffolding the new web: Standards and standards policy for the digital economy*. Santa Monica, CA: Rand.
- Lipton, M. (1996). Opinion: Demystifying the development of an organizational vision. *MIT Sloan Management Review*, 37(4), 83–92.
- Litzelman, D., Dittus, R., Miller, M., & Tierney, W. (1993, June). Requiring physicians to respond to computerized reminders improved their compliance with preventive care protocols. *Journal of General Internal Medicine*, 8, 311–317.
- Logical Observation Identifiers Names and Codes. (2004). *LOINC background*. Retrieved November 2004 from <http://www.loinc.org/background>
- Low, D., & Belcher, J. (2002). Reporting medication errors through computerized medication administration. *Computers, Informatics, Nursing*, 20(5), 178–183.
- MacDonald, K. (2003). *Online patient-provider communication tools: An overview*. Oakland, CA: California HealthCare Foundation.
- Marotta, D. (2000). *Healthcare informatics: HL7 in the 21st century*. Retrieved March 4, 2004, from http://www.healthcare-informatics.com/issues/2000/04_00/h17.htm
- Marshall, P., & Chin, H. (1998). *The effects of an electronic medical record on patient care: Clinician attitudes in a large HMO*. Paper presented at the annual AMIA symposium, Portland, OR.
- Massaro, T. A. (1993a). Introducing physician order entry at a major academic medical center: I. Impact on organizational culture and behavior. *Academic Medicine*, 68(1), 20–25.
- Massaro, T. A. (1993b). Introducing physician order entry at a major medical center: II. Impact on medical education. *Academic Medicine*, 68(1), 25–30.
- May, S. (2002). A CPR system can grow a practice: Improved efficiencies in charting and workflow allow better and faster healthcare delivery. *Healthcare Informatics*, 19(1), 93–94.
- McAfee, A. (2003). When too much IT knowledge is a dangerous thing. *MIT Sloan Management Review*, 44(2), 83–89.
- McDonald, C., Hui, S., Smith, D., Tierney, W., Cohen, S., Weinberger, M., et al. (1984). Reminders to physicians from an introspective computer medical record: A two-year randomized trial. *Annals of Internal Medicine*, 100, 130–138.
- McDowell, S., Wahl, R., & Michelson, J. (2003). Herding cats: The challenges of EMR vendor selection. *Journal of Healthcare Information Management*, 17(3), 63–71.
- McKenney, J., Copeland, D., & Mason, R. (1995). *Waves of change: Business evolution through information technology*. Boston: Harvard Business School Press.
- McPhee, S., Bird, J., Fordham, D., Rodnick, J., & Osborn, E. (1991). Promoting cancer prevention activities by primary care physicians: Results of a randomized, controlled trial. *Journal of the American Medical Association*, 266, 538–544.
- McPhee, S., Bird, J., Jenkins, C., & Fordham, D. (1989). Promoting cancer screening: A randomized, controlled trial of three interventions. *Archives of Internal Medicine*, 149, 1866–1872.
- Medical Records Institute. (2004a). *Continuity of Care (CCR): The concept paper of the CCR—Version 3*. Retrieved July 21, 2004, from <http://www.medrecinst.com/pages/about.asp?id=54>
- Medical Records Institute. (2004b). *Healthcare documentation: A report on information capture and report generation*. Boston: Author.
- Medical Records Institute. (2004c). *Survey of electronic health record trends and usage for 2004*. Boston: Author.

- Mendelson, D. (2003, December 7). *Financial incentive programs for health information technology: Lessons learned*. Paper presented at the eHealth Initiative Summit, Washington, DC. Retrieved November 2004 from www.ehealthinitiative.org
- Metzger, J., & Fortin, J. (2003). *Computerized physician order entry in community hospitals: Lessons from the field* (California HealthCare Foundation and First Consulting Group). Retrieved August 2004 from <http://www.chcf.org/documents/hospitals/CPOECommHospCorrected.pdf>
- Metzger, J., & Turisco, F. (2001). *Computerized physician order entry: A look at the marketplace and getting started*. Washington, DC, and New York: Leapfrog Group and First Consulting Group.
- Miller, R., Hillman, J., & Given, R. (2004). Physician use of IT: Results from the Deloitte Research Survey. *Journal of Healthcare Information Management*, 18(1), 72–80.
- Miller, R., & Sim, I. (2004). Physicians' use of electronic medical records: Barriers and solutions. *Health Affairs*, 23(2), 116–126.
- Miller, R., Sim, I., & Newman, J. (2003). *Electronic medical records: Lessons from small physician practices*. Oakland, CA: California HealthCare Foundation.
- Moyer, C., Stern, D., Dobias, K., Cox, D., & Katz, S. (2002, May). Bridging the electronic divide: Patient and provider perspectives on e-mail communication in primary care. *American Journal of Managed Care*, pp. 427–433.
- myPHR. (2004). *What is a health record?* Retrieved November 2004 from <http://www.myphr.com/whatis/index.asp>
- National Center for Health Statistics. (2004). *Classifications of diseases and functioning and disability*. Retrieved November 2004 from <http://www.cdc.gov/nchs/icd9.htm>
- National Committee for Quality Assurance. (2004). *Measuring the quality of America's healthcare*. Retrieved July 20, 2004, from <http://www.ncqa.org>
- National Committee on Vital and Health Statistics. (2001). *Information for health: A strategy for building the National Health Information Infrastructure*. Retrieved December 2004 from <http://aspe.hhs.gov/sp/nhii/Documents/NHIIReport2001/default.htm>
- National Committee on Vital and Health Statistics. (2003, November 5). *Letter to the secretary: Recommendations for PMRI terminology standards*. Retrieved December 2004 from <http://www.ncvhs.hhs.gov/031105lt3.pdf>
- National Council for Prescription Drug Programs. (2004). *Basic guide to standards*. Scottsdale, AZ: Author.
- National Electrical Manufacturers Association. (2003). *Digital imaging and communications in medicine (DICOM), Part 1: Introduction and overview*. Rosslyn, VA: Author.
- National Library of Medicine. (2003). *Fact sheet: Unified Medical Language System*. Retrieved March 3, 2004, from <http://www.nlm.nih.gov/pubs/factsheets/umls.html>
- National Uniform Billing Committee. (1999). *The history of the NUBC*. Retrieved July 20, 2004, from <http://www.nubc.org/history.html>
- Office of Personnel Management. (2002). *Federal Employees Health Benefit Program: HEDIS quality measures*. Retrieved July 20, 2004, from <http://www.opm.gov/insure/health/hedis2002>
- Ornstein, S., & Bearden, A. (1994). Patient perspectives on computer-based medical records. *Journal of Family Practice*, 38(6), 606–610.
- Ornstein, S., Garr, D., Jenkins, R., Rust, P., & Arnon, A. (1991). Computer-generated physician and patient reminders: Tools to improve population adherence to selected preventive services. *Journal of Family Practice*, 32(1), 82–90.
- Overhage, J. M., Dexter, P. R., Perkins, S. M., Cordell, W. H., McGoff, J., McGrath, R., et al. (2002). A randomized, controlled trial of clinical information shared from another institution. *Annals of Emergency Medicine*, 39(1), 14–23.

- Overhage, J., Tierney, W., Zhou, X., & McDonald, C. (1997). A randomized trial of "corollary orders" to prevent errors of omission. *Journal of the American Medical Informatics Association*, 4(5), 364–375.
- Oz, E. (2000). Controls and security measures. In E. Oz, *Management information systems* (pp. 618–659). Boston: Course Technology.
- Oz, E. (2004). *Management information systems: Instructor edition* (4th ed.). Boston: Course Technology.
- Pastore, R. (2003, February 1). Cruise control. *CIO*. Retrieved December 2004 from <http://www.cio.com/archive/020103/overview.html>
- Poon, E., Blumenthal, D., Jaggi, T., Honour, M., Bates, D., & Kaushal, R. (2004). Overcoming barriers to adopting and implementing computerized physician order entry systems in U.S. hospitals. *Health Affairs*, 23(4), 184–190.
- Porter, M. (1980). *Competitive strategy*. New York: Free Press.
- Porter, M. (2001). Strategy and the Internet. *Harvard Business Review*, 79(3), 63–78.
- Quinsley, C. A. (2004). A HIPAA security overview (AHIMA Practice Brief). *Journal of AHIMA*, 75(4), 56A–56C.
- Raymond, B., & Dold, C. (2002). *Clinical information systems: Achieving the vision*. Oakland, CA: Kaiser Permanente Institute for Health Policy.
- Renner, K. (1996). Cost-justifying electronic medical records. *Healthcare Financial Management*, 50(10), 63–64, 66, 68, 70.
- Ridsdale, L., & Hudd, S. (1994). Computers in the consultation: The patient's view. *British Journal of General Practice*, 44, 367–369.
- Rob, P., & Coronel, C. (2004). *Database systems: Design, implementation, and management* (6th ed.). Boston: Course Technology.
- Ross, J., & Beath, C. (2002). Beyond the business case: New approaches to IT investment. *MIT Sloan Management Review*, 43(2), 51–59.
- Ross, J., Beath, C., & Goodhue, D. (1996). Develop long-term competitiveness through IT assets. *MIT Sloan Management Review*, 38(1), 31–42.
- Safeware, The Insurance Agency, Inc. (2003). *Safeware's 2002 PC loss survey shows big increase in accidental damage claims*. Retrieved July 21, 2004, from <http://www.safeware.com/pressrelease3-17-03.htm>
- Sambamurthy, V., & Zmud, R. (1996). *Information technology and innovation: Strategies for success*. Morristown, NJ: Financial Executives Research Foundation.
- Schott, S. (2003, April). How poor documentation does damage in the courtroom. *Journal of AHIMA*, 74(4), 20–24.
- Severance, D., & Passino, J. (2002). *Making I/T work*. San Francisco: Jossey-Bass.
- Shakir, A. (1999). Tools for defining data. *Journal of AHIMA*, 70(8), 48–53.
- Sittig, D., & Stead, W. (1994). Snap-shot of CHIME: Physician order entry. *Healthcare Informatics*, 11(10), 38.
- Smith, H. (2001). *A context-based access control model for HIPAA privacy and security compliance* (SANS Institute, Information Security Reading Room). Retrieved December 2004 from <http://www.sans.org/rr/whitepapers/legal/44.php>
- SNOMED International. (2004). *SNOMED CT: Comprehensive, worldwide clinical terminology*. Retrieved November 2004 from www.snomed.org
- Solomon, G., & Dechter, M. (1995). Are patients pleased with computer use in the examination room? *Journal of Family Practice*, 41(3), 241–244.
- Spurr, C. (2003). *Information systems project management at Partners HealthCare System*. Internal document, Partners HealthCare System, Inc.

- Stair, R., & Reynolds, G. (2003). *Principles of information systems* (6th ed.). Boston: Course Technology.
- Standards for privacy of individually identifiable health information*. (2001). HIPAAAdvisory. Retrieved June 28, 2004, from <http://www.hipaadvisory.com/regs/finalprivacy/gwhole.htm>
- Strassman, P. (1990). *The business value of computers*. New Canaan, CT: Information Economics Press.
- Superior Consultant Company. (2004). *Best strategies for selecting a clinical information system*. Dearborn, MI: Author.
- Tate, K., Gardner, R., & Weaver, L. (1990). A computerized laboratory alerting system. *M.D. Computing*, 7(5), 296–301.
- Taylor, H., & Leitman, R. (2002). Patient/physician online communication: Many patients want it, would pay for it, and it would influence their choice of doctors and health plans. *Health Care News*, 2(8), 1–4.
- Teich, J., Merchia, P., Schmiz, J., Kuperman, G., Spurr, C., & Bates, D. (2000). Effects of computerized physician order entry on prescribing practices. *Archives of Internal Medicine*, 160, 2741–2747.
- Tierney, W., McDonald, C., Hui, S., & Martin, D. (1988). Computer predictions of abnormal test results. *Journal of the American Medical Association*, 259, 1194–1198.
- Tierney, W., Miller, M., & McDonald, C. (1990). The effect on test ordering of informing physicians of the charges for outpatient diagnostic tests. *New England Journal of Medicine*, 322, 1499–1504.
- Tierney, W., Miller, M., Overhage, J., & McDonald, C. (1993). Physician inpatient order writing on microcomputer workstations: Effects on resource utilization. *Journal of the American Medical Association*, 269, 379–383.
- Toole, J. (2003). The need for transformation. In *Health Care Technology* (Vol. 1). San Francisco: Montgomery Research.
- University of Kansas Medical Center. (2004). *Kansas University Center for TeleMedicine & TeleHealth*. Retrieved November 2004 from <http://www2.kumc.edu/telemedicine>
- University of Texas Medical Branch. (2004). *UTMB Center for Telehealth*. Retrieved November 2004 from <http://www.utmb.edu/telehealth>
- Van Hentenryck, K. (1998). *Health Level Seven: A standard for health information systems*. Retrieved March 4, 2004, from <http://www.medicalcomputingtoday.com/0oph17.html>
- Waagemann, C. (1995). The five levels of the ultimate electronic medical record. *Health Care Informatics*, 12, 26–35.
- Waagemann, C. (1996). The five levels of electronic health records. *M.D. Computing*, 13(3), 199–203.
- Wager, K., Lee, F., White, A., Ward, D., & Ornstein, S. (2000). Impact of an electronic medical record system on community-based primary care practices. *Journal of the American Board of Family Practice*, 13(5), 338–348.
- Walsh, T. (2003). Best practices for compliance with the final Security Rule. *Journal of Healthcare Information Management*, 17(3), 14–18.
- Wang, S., Middleton, B., Prosser, L., Bardon, C., Spurr, C., Carchidi, P., et al. (2003). A cost-benefit analysis of electronic medical records in primary care. *American Journal of Medicine*, 114, 397–403.
- Webopedia. (2004a). *Audit trail*. Retrieved November 2004 from http://www.webopedia.com/TERM/a/audit_trail.html

- Webopedia. (2004b). *The seven layers of the OSI model*. Retrieved November 2004 from http://www.webopedia.com/quick_ref/OSI_Layers.asp
- Webopedia. (2004c). *Token-ring network*. Retrieved November 2004 from http://www.webopedia.com/TERM/T/token_ring_network.html
- Weil, S. (2004). *The final HIPAA Security Rule: Conducting effective risk analysis*. Retrieved April 13, 2004, from <http://www.hipaadvisory.com/action/Security/riskanalysis.htm>
- Weill, P., & Broadbent, M. (1998). *Leveraging the new infrastructure*. Boston: Harvard Business School Press.
- Weill, P., & Ross, J. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Boston: Harvard Business School Press.
- Whatis?com. (2002). *The Whatis?com encyclopedia of technology terms*. Indianapolis, IN: Que.
- White, C. (2001). *Data communications and computer networks: A business user's approach*. Boston: Course Technology.
- Whitten, J., Bentley, L., & Dittman, K. (2004). *Systems analysis and design methods* (6th ed.). New York: McGraw-Hill/Irwin.
- Wise, P., & Mon, D. (2004). *EHR functional outline review & validation*. Retrieved October 2004 from <http://www.hl7.org/ehr/documents/public/presentations/18>
- Yarnall, K., Rimer, B., Hynes, D., Watson, G., Lyna, P., Woods-Powell, C., et al. (1998). Computerized prompts for cancer screening in a community health center. *Journal of the American Board of Family Practice*, 11(2), 96–104.

Index

A

- Aarts, J., 168
- Access: physical control of, 259, 266; technical control of, 260, 267–269
- Accessibility of data, 50, 55
- Accreditation: by Accreditation Association for Ambulatory Care (AAHC), 74; by American Osteopathic Association (AOA), 73–74; benefits of, 65; by Commission on Accreditation of Rehabilitation Facilities (CARF), 74; by Joint Commission on Accreditation of Healthcare Organizations (JCAHO), 64, 65–66; by National Committee for Quality Assurance (NCQA), 72–73; overview of, 65
- Accreditation Association for Ambulatory Care (AAHC), 74
- Accreditation Association for Ambulatory Health Care (AAHC), 74
- Accredited Standards Committee (ASC), X12N standards, 235, 242–243
- Accuracy of data, 50, 55
- Acquisition. *See* System acquisition
- Ad hoc standards, 234
- Addressable specifications, HIPAA Security Rule, 257
- Administration, IT, as function of IT department, 284–285
- Administrative information systems, 92, 94–95
- Administrative safeguards, 261–265; chief security officers as, 258, 263–264; HIPAA Security Rule standards on, 257–259; risk analysis and management as, 258, 262–263; system security evaluation as, 259, 264–265
- Admission/discharge records, 9
- Adverse drug events, 124
- Agarwal, R., 309, 312
- Agency for Healthcare Quality and Research, 126
- Aggregate data and information: administrative, 28–29, 30; clinical, 27–28; combining clinical and administrative, 29, 31
- Alignment. *See* IT strategy and alignment
- Altis, Inc., 191
- Amatayakul, M., 75
- Ambulatory care: benefits of CPOE systems in, 126–127; scope of episode of care in, 16; Uniform Ambulatory Care Data Set (ACDS), 19, 21
- American Academy of Pediatrics (AAP), 244
- American College of Physicians, 65
- American College of Radiology (ACR), 241
- American College of Surgeons, 65
- American Health Information Management Association (AHIMA), 81, 243; on content of patient medical records, 8–11; data quality management model, 49–57; guidelines on legal health record, 75–79; on HIPAA standards, 256, 257; overview of, 458; on retention of and destruction of health records, 79–80
- American Hospital Association (AHA), 17, 65

- American Medical Association (AMA), 243; Current Procedural Terminology (CPT) published by, 21, 23, 25, 26; and formation of JCAHO, 65; NUCC formed by, 17; on-line communication guidelines of, 137–138
- American Medical Informatics Association (AMIA), 153, 243, 458
- American National Standards Institute (ANSI): bar code standard of, 220; standards development process of, 235, 236
- American Nurses Association (ANA), 243
- American Osteopathic Association (AOA), 73–74
- American Telemedicine Association, 105, 142–143
- Antivirus software, 275–276
- Applegate, L., 366, 367, 368, 369
- Application program interface (API), 194
- Application service providers (ASPs), 158–159, 304
- Applications: as component of IT asset, 326; integration of, 228; “killer,” 356–357, 358; management of, as function of IT department, 283–284; outsourcing development of, 304; visionary, 375–376
- Applications programmers, 289
- Applications software, 190
- Architecture. *See* Information systems architecture
- Arden Syntax for Medical Logic Systems, 241
- Arnon, A., 119
- ARPANET, 211
- Artificial intelligence (AI), 216–217
- Arts, D., 57–58
- Ash, J., 126, 169
- Assembly languages, 190
- Associated Press, 252
- Asynchronous Transfer Mode (ATM), 204
- Atomicity of data, 53, 56–57
- Audit trails, 272
- Audits, postimplementation, 435–437
- Austin, R., 366, 367, 368, 369
- Authentication: entity, 261, 269–272; of patient medical records, 74, 80–81
- Authority: clarified by governance mechanisms, 363–364; deemed, 64, 65, 74
- Authorization forms: overview of, 85–88; in patient medical records, 10–11, 14; vs. consent forms, 87–88
- Automated medical records, 113
- Automatic log-off, 260, 269
- ## B
- Baggage, organizational: created by competition, 357–359; as reason for IT initiative failure, 409
- Baker, L., 104
- Balanced scorecards, 32
- Balas, D., 119
- Bandwidth, 206, 208–209
- Bar coding, 108, 219–220, 348–349
- Barcode-enabled point of care (BPOC) medication administration systems, 131–132, 220
- Barlas, S., 132
- Barlow, S., 120
- Bates, D., 119, 120, 124, 126, 129, 131, 143, 420
- Bazzoli, E., 233
- Bearden, A., 121
- Beath, C., 354, 377, 422
- Belcher, J., 131
- Benchmarking, 31–32, 438
- Bensaou, M., 339
- Bentley, L., 92, 173
- Berg, M., 168
- Berkman, E., 346
- Berman, J., 119
- Bertram, D., 112
- Best-of-breed architecture, 228, 230–231
- Billing: as focus of early health care information systems, 93, 95; as purpose for patient medical records, 8; standard forms for, 17, 18–19, 20. *See also* Reimbursement
- Biometric identification systems, 271
- Bird, J., 119
- Bits per second (bps), 209
- Bleich, H., 120
- Bluetooth, 204
- Blumenthal, D., 119, 143
- Board of directors, IT responsibilities of, 370–371
- Bond, C., 131
- Books, health care industry, 457
- Boren, S., 119
- Brailer, D., 118, 125
- Bresnahan, J., 445
- Briceland, L., 131
- Bridges, network, 209
- Briney, A., 153, 252, 254, 270, 271
- Broadbent, M., 339, 377, 379, 444
- Brown, C., 373
- Brown, G., 119
- Brown, J., 446
- Brown, N., 132, 133, 142
- Budgets. *See* IT budgets
- Bundorf, M. K., 104
- Burke, J., 119
- Burnum, J., 112
- Bus typology, 205–206
- Bush, G. W., 248
- Business owners, project management, 398
- Business sponsors, project management, 397–398, 399
- ## C
- California HealthCare Foundation, 81, 134, 180
- Capital budgets, 384
- Capitated reimbursement, 100
- Carr, N., 446
- Carriers, telecommunications, 208
- Cash, J., 355, 408, 411
- Cathode ray tube (CRT) technology, 221
- Catizone, C., 131
- Cecil, J., 352
- Census statistics, 29
- Center for Healthcare Information Management (CHIM), 459
- Centers for Medicare and Medicaid Services (CMS), 85, 88, 256; aggregate data from, 17, 38, 39; CMS-1500 form of, 17, 20; deemed authority given by, 64, 65, 74
- Certification, Medicare and Medicaid, 62, 64
- Champy, J., 173
- Change. *See* Organizational change
- Chief executive officers (CEOs), 287, 382–383

- Chief financial officers (CFOs),
CIOs reporting to, 287
- Chief information officers (CIOs):
CTO duties handled by, 287;
and IT departmental organization, 299–300; and IT effectiveness, 376, 378, 379, 380, 381;
job description for, 290–291; responsibilities of, 285–287, 288;
strategic discussion role of, 331, 332, 333, 336; telecommunications function managed by, 284
- Chief medical informatics officers (CMIOs), 151, 287–288, 292–294
- Chief operating officers (COOs), 287
- Chief security officers (CSOs), 258, 263–264, 287, 288
- Chief technology officers (CTOs), 287, 288
- Chin, H., 121
- Chin, T., 128
- Christensen, C., 353, 358
- Cimino, J., 234, 242
- Ciphertext, 273
- Classen, D., 119
- Client/server systems, 210
- Clinical Context Management (CCM) standards, 241
- Clinical data repositories, 198
- Clinical information systems: barriers to adoption of, 141–144;
common types of, 94–95, 111;
critical success factors in implementing, 415; defined, 92–93;
EMR as “hub” of, 137, 140. *See also* System acquisition; System implementation
- Clinical research and outcomes analysis, and poor-quality documentation, 47
- Clinton, B., 103
- CMS-1450. *See* UB-92
- CMS-1500, 17, 20
- Coaxial cable, 208
- Coding: as basis for DRG determination, 23; standards for, 25; systems for, 21, 23–25, 26
- College of Healthcare Information Management Executives (CHIME), 240, 243, 285–286, 459
- Collins, J., 354–355, 447
- Commission on Accreditation of Rehabilitation Facilities (CARF), 74
- Committee on Workforce Needs in Information Technology, 296
- Committee to Study the Impact of Information Technology on the Performance of Service Activities, 422, 444
- Common Criteria, 264–265
- Communication: data, 200; and failure of IT initiatives, 410; network, devices and protocols for, 201–204, 209; of progress in IT initiatives, 176–177, 412–413; as purpose for patient medical records, 8; in system acquisition process, 163; in system implementation, 176–177; of value of IT investments, 438. *See also* Electronic mail (e-mail)
- Compact disks (CDs), 222
- Comparative data and information, 31–40
- Competition, IT strategies based on views about, 323–325
- Competitive advantage, IT-enabled, 342–359; baggage created by pursuit of, 357–359; continuous and multiple initiatives for, 356–357, 358; examples of companies with, 343–346; factors limiting, 354–356; sources of advantage with, 346–351; sustaining, 351–354, 377–378
- Competitive forces model, 324
- Comprehensiveness of data, 51, 55
- Computer networks. *See* Networks
- Computer Sciences Corporation, 339
- Computer-based patient records (CPRs): IOM definition of, 102–103, 112; rate of adoption of, 103. *See also* Electronic medical record (EMR) systems
- Computer-Based Patient Records* (Institute of Medicine), 102–103, 112
- Computer-Based Patient Records Institute (CPRI), Nicholas E. Davies Award, 121, 122, 123
- Computerized medical record systems, 113–114, 117. *See also* Document imaging systems
- Computerized provider order entry (CPOE) systems, 122, 124–130; benefits of, 126–127; defined, 124–125; patient safety improved by, 106, 124, 126, 420; physician resistance to, 179–180; problems in implementing, 127–130; rates of usage of, 125–126; sample screen from, 125; setting goal of implementing, 170; training for, 175–176
- Computers: external storage devices for, 221–222, 223; input devices for, 218–220; laptop computers, 223, 224; mainframe, 95–96, 98; microcomputers, 100–101, 104; minicomputers, 96–97, 99; output devices for, 221; personal digital assistants (PDAs), 107, 225; smart phones, 225; tablet computers, 223, 224
- Conditions of Participation (CoPs), 64
- Confidentiality, 81–83; defined, 81; of drug and alcohol treatment records, 83; as factor in lag in health care IT use, 108; federal laws on, 82–85; recent breaches of, 82
- Consensus-based standards, 234–235
- Consent forms: in patient medical records, 10, 14; vs. authorization forms, 87–88
- Consistency of data, 51, 55
- Consultants, IT services evaluation, 305
- Consultation notes/reports, 10
- Context-based access, 268
- Continuity of Care Record (CCR) standard, 244–245
- Contracting: with application service providers (ASPs), 158–159; with system developers, 159
- ConWay Transportation Services, Inc., 343–344
- Copeland, D., 356, 357, 378, 381
- Core processes, IT strategies based on improvement of, 320–321, 322
- Coronel, C., 192
- Cost savings: with adoption of electronic transactions under HIPAA, 103; with CPOE systems, 127; with electronic

medical records (EMRs), 120;
IT investments for, 424
Cost-based reimbursement, 93
Cost-benefit analysis, system acquisition, 161–162
Costs, health care: for documentation, 47; methods of containing, 99–100
Court cases, poor-quality documentation's consequences for, 46
Covered entities (CEs): HIPAA Privacy Rule, 84, 256; HIPAA Security Rule, 257
Cox, D., 104
Cruz, G., 306, 450
Cryptography, 272
Currency of data, 52, 55
Current Procedural Terminology (CPT), 21, 25, 26

D

Data: clean, 176, 198; as component of IT asset, 327; rapid and accurate provision of, 348–349; standards for interchange or integration of, 239–243. *See also* Health care data
Data communications, 200. *See also* Networks
Data conversion, system implementation, 176
Data definition language (DDL), 193–194
Data dictionaries, 198
Data encryption, 260, 261, 272–274, 276
Data manipulation language (DML), 194
Data manipulation layer, 194
Data marts, 200
Data mining, 200
Data modeling, relational, 194–197
Data warehouses, 198, 199–200
Database administrators, 289, 291
Database management systems: object-oriented (OODBMSs), 197; object-relational (ORDBMSs), 197; relational (RDBMSs), 193–194
Databases, 192–200; clinical data repository, 198; data dictionaries for, 198; data mart, 200; data mining of, 200; data warehouse,

198, 199–200; information processing distribution schemes for, 210; object-oriented (OODBs), 192, 197; object-relational (ORDBs), 192; on-line transactional processing (OLTP), 198–199; relational (RDBs), 192–197
Davenport, T., 173
Davies Award, 121, 122, 123
Davis, G., 99
De facto standards, 234
DeBor, G., 420
Dechter, M., 121
Decision making: IT governance, archetypes of, 374; steps in process of, 215; support systems for, 215–218; and types of problems, 215
Decision-support systems (DSS), 216, 323
Deemed authority, 64, 65, 74
Definitions of data, 52, 55–56
DeKeizer, N., 57–58
DeLuca, J., 157, 301
Department of Defense, *Trusted Computer System Evaluation Criteria* (TCSEC), 264
Department of Health and Human Services (HHS), 103, 246, 247, 248; Office of Inspector General (OIG), 25
Department of Labor, Bureau of Labor Statistics, 289, 291
Designated standard maintenance organizations (DSMOs), 246
Destruction of patient medical records, 79–80
Deuser, J., 134
Diagnosis related groups (DRGs): ICD-9-CM coding as basis of, 23; Medicare reimbursement system based on, 99–100
Digital Imaging and Communications in Medicine (DICOM) standard, 234, 241–242
Digital video disks (DVDs), 222
Disaster notification systems, 421
Discharge statistics, 29
Discharge summaries, 11, 14
Disease and procedure indexes, 27, 28
Disease management programs, 102
Disk drives, 221

Dittman, K., 92, 173
Dittus, R., 119
Dobias, K., 104
Document imaging systems: advantages and disadvantages of, 220; computerized medical record systems as, 113–114, 117; financial analysis of, 428; IT value of, 421
Documentation. *See* Health care documentation
Dold, C., 102, 119
Domain Name System (DNS) servers, 212
Domain names, 213, 214
Donald, J., 120
Doorewaard, H., 168
Downes, L., 356
Dragoon, A., 433
Drazen, E., 362
Drug and alcohol treatment records, confidentiality of, 83
Duxbury, B., 119
Dvorak, R., 381–382
Dykstra, R., 169

E

e-mail. *See* Electronic mail (e-mail)
e-procurement systems, 421
Earl, M., 286, 339, 340, 382
Effectiveness. *See* IT effectiveness
Efficiency, electronic medical records (EMRs), 120
eHealth Initiative, 243, 248
EHR Collaborative, 243
Electronic data interchange (EDI), 210, 420
Electronic health records (EHRs), 116, 117; Continuity of Care Record (CCR) standard, 244–245; EHR Functional Model and Standard, 241, 243–244. *See also* Electronic medical record (EMR) systems
Electronic mail (e-mail), 104; advantages of using, 135; current use for physician-patient communication, 135; policies and guidelines on, 136–137, 138–139; problems in using, 136; protocols for, 214
Electronic medical record (EMR) systems, 112–121; barriers to

- Electronic medical record (EMR) systems (*continued*)
 adopting, 141–144; benefits of, 119–121; and computer-based patient records (CPRs), 102–103, 112; Davies Award for implementing, 121, 122, 123; EMRs defined, 112, 114–116, 117; example of acquisition of, 148–150; as “hub” of clinical information systems, 137, 140; and levels of computerization of patient health information, 112–117; rates of usage of, 103, 118; reasons for adoption of, 118–119; sample screens from, 11, 115; setting goal of implementing, 170–171; value of, 420. *See also* Electronic health records (EHRs); Patient medical records
- Electronic medical records (EMRs). *See* Electronic medical record (EMR) systems
- Electronic patient records, 116
- Electronic signatures, 80–81
- Encoders, 25
- Encryption, 260, 261, 272–274, 276
- Encryption algorithm, 273
- Eng, J., 272
- Enmark, R., 157, 301
- Enterprise Rent-a-Car, 345–346
- Entity authentication: automatic log-off for, 260, 269; common methods for, 269–272; defined, 269; HIPAA Security Rule standard on, 261; unique identifiers for, 260, 269
- Entity relationship diagrams (ERDs), 194–197
- ePHI, 256
- Etheridge, Y., 274
- Ethernet, 204, 205, 207
- Evaluation: of effectiveness of IT services, 305–312; of governance, 306; of system acquisition, 306; of system implementation, 307; of system security, 259, 264–265; of vendor proposals, 159–161, 442
- Evans, J., 120
- Evans, R., 119, 124
- Executive information systems (EISs), 216
- Expert systems, 217
- Extensible markup language (XML): and current standards, 240, 242, 244; defined, 212, 213; as messaging standard of future, 233, 234
- External storage devices, 221–222, 223
- Extranets, 215
- ## F
- Face sheets, 9
- Failure: to deliver returns on IT investments, 438–443, 444; of IT initiatives, 407–414
- Fairchild, D., 120
- Fee-for-service reimbursement, 100
- Feeney, D., 286, 382
- Feld, C., 368
- Fiber-optic cable, 208
- File server systems, 210
- File Transfer Protocol (FTP), 214
- Financial analyses, IT project proposals, 426–427, 428
- Financial barriers, adoption of clinical information systems, 141–143
- Firewalls, 274–275
- First Consulting Group, 124, 125, 180
- Fiskio, J., 120
- Flash memory, 222, 223
- Fluke Networks, 276
- Fordham, D., 119
- Fortin, J., 175, 180
- Fournier, L., 126, 169
- Fourth generation languages (4GLs), 190
- Freedman, D., 355
- Freedom of Information Act (FOIA), 83
- Frelinger, D., 235
- Fundamental change, 393
- Fuzzy logic, 218
- ## G
- Gadd, C., 121
- Gandhi, T., 119
- Gantt charts, 163, 164
- Garb, C., 119
- Gardner, R., 120
- Garr, D., 119
- Garrett, L., Jr., 120
- Gateways, network, 209
- Gawande, A., 119, 120, 124
- Given, R., 135
- Glaser, J., 227, 308–309, 420, 433
- Goals: of IT investment, 441–442; of system acquisition, 151–152, 153; of system implementation, 170–171
- Goldsmith, J., 103, 104
- Goldstein, M., 352
- Goodhue, D., 354, 377
- Gopalakrishna, R., 272
- Gorman, P., 126
- Governance. *See* IT governance
- Governing concepts, 328–330
- Government mandates: as reason for IT investments, 423–424; standards established by, 234
- Granularity of data, 53, 56–57
- Gue, D., 256, 257
- ## H
- Haddad, S., 121
- Hagel, J., 446
- Hammer, M., 173
- Hammond, W., 120, 234, 242
- Hankin, R., 220
- Harrah's Entertainment, 344–345
- Hatoum, H., 131
- Hayashi, A., 120
- Health care: costs of, 47, 99–100; reasons for lag in IT use by, 108–109
- Health care data: characteristics of, for quality management, 50–57; errors in, 57–58, 59; needed to process reimbursement claims, 16–17, 18–19, 20; vs. health care information, 44–45. *See also* Data
- Health care data quality, 43–60; activities for improving, 59; AHIMA model of, 49–57; consequences of poor, 45–47; data errors and, 57–58; example of importance of, 60; MRI principles for ensuring, 48
- Health care documentation: consequences of poor-quality, 45–47; costs of, 47; legal status of, 8; MRI principles of, 48; parts of, 47. *See also* Patient medical records

- Health care information: complexity of, 108; defined, 4–5; types of, 5–7; vs. health care data, 44–45
- Health care information systems (HCISs): categories of, 92–93, 94–95; defined, 92; history and evolution of, 93, 95–108. *See also* Clinical information systems; System acquisition; System implementation
- Health care information systems standards. *See* Standards
- Health care IT industry, 449–460; major vendors in, 454–455; market structure of, 452–453; professional associations in, 457–460; publications on, 455–457; research firms in, 457; size of, 450–452
- Health care knowledge, defined, 44, 45
- Health care organizations, defined, 92
- Health care statistics, 29
- Health Industry Bar Code (HIBC) standard, 220
- Health Industry Business Communications Council (HIBCC), 220
- Health information. *See* Health care information
- Health Insurance Portability and Accountability Act (HIPAA): health information definition of, 4; and history of health care information systems, 103–104; impact on health care information standards, 234, 246–247; overview of, 83–84; Privacy Rule, 82–83, 84–85; Security Rule, 256–261
- Health Level Seven (HL7) standards, 235, 240–241; EHR Functional Model and Standard, 241, 243–244
- Health Plan Employer Data and Information Set (HEDIS): overview of, 32–35; report cards using data from, 35–37
- Health Privacy Project, 81, 82
- Health records. *See* Patient medical records
- Healthcare Common Procedural Coding System (HCPCS), 25, 26
- Healthcare Information and Management Systems Society (HIMSS), 126, 153, 304; Bar Coding Task Force, 131, 132; Davies Award, 121, 122, 123; and health record content standards, 243, 244; overview of, 459
- HealthGrades, 40
- Heda, S., 99
- HEDIS. *See* Health Plan Employer Data and Information Set (HEDIS)
- Henderson, J., 315
- Hershey, C., 112
- Herzlinger, R., 342
- HHS. *See* Department of Health and Human Services (HHS)
- Hill-Burton Act, 93
- Hillman, J., 135
- HIPAA. *See* Health Insurance Portability and Accountability Act (HIPAA)
- History and physical, 9, 14
- Holen, E., 381–382
- Honour, M., 143
- Horsky, J., 120
- Hospital Corporation of America (HCA), 109
- Hospital Survey and Construction Act, 93
- Hospitals: deaths due to medical errors made in, 122, 124; evolution of Medicare reimbursement to, 93, 99–100; JCAHO-accredited, and federal accreditation standards, 64; patient medical records generated from admissions to, 12–14; scope of episode of care with stay in, 16
- Hubs, network, 206, 209
- Hudd, S., 121
- Hughes, G., 277
- Hui, S., 120
- Hulkower, S., 119
- Hutchinson, R., 131
- Hypertext markup language (HTML), 212, 213
- Hypertext Transfer Protocol (HTTP), 212, 213, 214
- I**
- IBM Token Ring, 205
- ICD-9-CM, 21, 23–25
- ICD-10-CM, 25
- Identification sheets, 9, 12
- IEEE 802.11 standards, 204, 276
- Imaging reports, 10
- Implementation. *See* System implementation
- Implementation team, system implementation, 168–169
- Incentives, and organizational change management, 395–396
- Incremental change, 392, 393–394
- Inertia, and IT initiative failure, 409
- Informatics officers, 151
- Information. *See* Health care information
- Information capture, 47
- Information management, JCAHO standards on, 67, 68
- Information systems (ISs): administrative, 92, 94–95; defined, 92; executive (EISs), 216; terminology, 92. *See also* Clinical information systems; Health care information systems (HCISs)
- Information systems architecture, 226–231; approaches to, 227–228; defined, 226–227; examples of, 228–229; terminology, 227; value of focus on, 229–231
- Information technology (IT): as commodity, 446–447; defined, 92; great companies' orientation to, 354–355; and history of health care information systems, 95–98, 99, 100–101, 104, 105, 107–108; infrastructure of, for system implementation, 182; maturity of, and failure of IT initiatives, 413–414; new, IT strategies based on role of, 321–322; reasons for health care's lag in use of, 108–109; reviewing new, 332–333, 335; standards for, 233–234, 235, 264–265; as tool, 354–356, 445. *See also* entries beginning with "IT"
- Infrastructure: information systems architecture, 227; IT, for system implementation, 182; as IT asset component, 327; IT investments for, 423; local healthcare information infrastructures (LHIIIs), 248; National Healthcare Information Infrastructure (NHII),

- Infrastructure (*continued*)
 247–248; Public Key Infrastructure (PKI), 272–274
- Input devices, 218–220
- Institute of Medicine (IOM): Committee on Data Standards for Patient Safety, 105–106, 114; *Computer-Based Patient Records*, 102–103, 112; and EHR Functional Model, 243; *Patient Safety*, 105–106; *To Err Is Human*, 105, 106, 122, 124
- Integrated delivery system (IDS): competitive advantage gained with, 352, 353; IT departmental organization with, 298–299; IT governance to support, 364–365
- Integrated services digital network (ISDN) services, 208
- Integration: application, by information system architecture, 228; data, standards for, 239–243; and lag in IT use in health care, 106–107, 108–109
- Interface engines, 191–192, 193
- Internal rate of return (IRR), 426–427, 428
- International Classification of Diseases: ICD-9-CM, 21, 23–25; ICD-10-CD, 25
- International Organization for Standardization (ISO), 235, 236, 264
- Internet: health care organizations' use of, 210–211, 213–214; and history of health care information systems, 104–105; overview of, 211–214. *See also* Electronic mail (e-mail)
- Internet Message Access Protocol (IMAP), 214
- Internet model, 201, 203
- Internet Protocols (IPs), 212, 214
- Internet telephoning, 214
- Intranets, 214–215
- IT. *See* Information technology (IT)
- IT asset: components of, 326–328; as critical for IT effectiveness, 381; defined, 318, 325–326; leveraging, for competitive advantage, 353–354
- IT budgets, 383–388; categories in, 384–386; development of, 386–388; evaluating, 306; in project charters, 468; strategies for reducing, 429–430
- IT committees, 370–371, 437
- IT departments, 282–304; attributes of, 303–304; centralization vs. decentralization of, 300–301; core competencies of, 301–303; core functions of, 283–285; organizational structure of, 297–300; responsibilities of, 282–283, 366–367. *See also* IT services; IT staff
- IT effectiveness: evaluating, 305–312; organizations with high level of, 375–382; senior leader's contribution to, 382–383; studies of, and return on IT investments, 443
- IT governance, 362–374; archetypes of, 374; characteristics of well-developed, 363–364; as component of IT asset, 328; defined, 362–363; evaluating effectiveness of, 306; IT department responsibilities for, 366–367; organization strategies linked to, 364–366; senior management's responsibility for, 368–370; structures for, 370–374, 437; users' responsibilities for, 367
- IT investments: diverse IT value of, 420–425; factors increasing value from, 379; increased accountability for results of, 435, 436; management actions to improve value from, 433–438; reasons for failure to deliver returns on, 438–443, 444; relationship between organizational performance and, 444–445; types of, 422. *See also* IT projects
- IT liaisons, 331–332, 372–373
- IT managers, project management responsibilities of, 399
- IT planning: application agenda resulting from, 316; objectives of, 314–315; in organizations with IT excellence, 340–341. *See also* IT strategy and alignment; Project plans
- IT projects: factors contributing to failure of, 407–414; sustained incremental vs. “big bang,” 356–357, 358, 446–447. *See also* IT investments; *entries beginning with “project”*
- IT services: evaluating effectiveness of, 305–312; in-house vs. outsourced, 304–305; and IT department organizational structure, 297–300
- IT staff: attributes of, 295–296; as component of IT asset, 327–328; and IT department organizational structure, 297–300; leadership roles/positions on, 285–288, 290–291, 292–294; as liaisons for strategic discussions, 331–332; recruitment and retention of, 296–297; responsible for technical support, 181–182; roles vs. functions of, 295; technical roles/positions on, 288–289, 291, 294–295. *See also* IT departments
- IT steering committees, 372
- IT strategy and alignment: areas requiring, 318; challenges of creating, 339–342; formulation of, 317; and governing concepts, 328–330; implementation of, 317; linked to organization strategy, 320, 439–440; normative approach to developing, 330–338; vectors for arriving at, 318–325
- IT value, 418–447; diversity of, 420–425; factors increasing, from IT investments, 379; failure of IT investments to return, 438–443, 444; management actions to improve realization of, 433–438; and project proposals, 425–433; significance of, 420; studies of, 444–447; tangible and intangible, 419–420
- IT-enabled competitive advantage. *See* Competitive advantage, IT-enabled

J

Jaggi, T., 143
 Jenkins, C., 119
 Jenkins, M., 131
 Jenkins, R., 119
 Johns, M., 44

Johnson, J., 120
 Johnson, L. B., 93
 Johnston, B., 134
 Johnston, D., 126, 127
 Joint Commission on Accreditation of Healthcare Organizations (JCAHO): accreditation by, 64, 65–66; authentication definition of, 80; formation of, 65; health care information categories of, 4–5; information management standards, 67, 68; knowledge-based information definition of, 40; ORYX initiative, 37–38; standards for content and maintenance of patient records, 67, 69–72
 Just-in-time training, 175–176

K

Kaiser Permanente, 134; Institute for Health Policy, 119
 Karson, A., 120
 Katz, S., 104
 Kaushal, R., 131, 143
 Keen, P., 347, 391, 394, 445
 Kelly, D., 32
 Kelly, P., 158, 159
 Kennedy, O., 99
 Keys, encryption systems, 273
 Kilbridge, P., 299
 Kittleson, B., 454
 Knowledge-based information, 40–41
 Kuperman, G., 119, 120, 129
 Kurtz, M., 240

L

Laboratory reports, 10
 Lake, K., 357
 Landis, S., 119
 Langberg, M. L., 128, 129
 Languages: markup, 212, 213; programming, 190–191, 194. *See also specific languages*
 Laptop computers, 223, 224
 LaTour, K., 19, 21
 Lavelle, M., 126
 Leadership: actions, to improve IT value realization, 433–438; contribution to IT effectiveness, 382–383; IT governance

responsibilities of, 368–370, 371–372; for managing organizational change, 394; support from, and failure of IT initiatives, 408–409. *See also specific leadership positions*
 Leapfrog Group, 40, 106, 124, 125
 Lee, F. W., 44, 120, 169, 197, 252, 262, 265, 267, 270
 Legal documentation, patient medical records as, 8
 Legal health record (LHR), AHIMA guidelines on, 75–79
 Legler, J., 121
 Legrow, G., 158, 159
 Leitman, R., 135
 Lesar, T., 131
 Levinson, M., 345
 Levit, K., 120
 Libicki, M., 235
 Licensure of facilities, 62, 63
 Linux, 191, 235
 Lipton, M., 342
 Liquid crystal display (LCD) technology, 221
 Litelman, D., 119
 Local area networks (LANs), 101, 205
 Local healthcare information infrastructures (LHIIs), 248
 Logical Observation Identifiers Names and Codes (LOINC), 238
 Low, D., 131
 Lyman, J., 126

M

MacDonald, K., 104, 134, 135, 136
 Machine languages, 190
 Mainframe computers, 95–96, 98
 Maintenance: following system implementation, 183; Web-site, 294–295, 304
 Managed care organizations (MCOs), NCQA accreditation of, 72, 73
 Management, of organizational change, 391–396. *See also Leadership*; Project management
 Mandates. *See* Government mandates
 Mark, D., 381–382
 Markup languages, 212
 Marotta, D., 240, 241
 Marshall, P., 121

Martin, D., 120
 Mason, R., 356, 357, 378, 381
 Massaro, T. A., 127
 May, S., 120
 McAfee, A., 415–416
 McAloon, M., 112
 McDonald, C., 119, 120
 McDowell, S., 147
 McFarlan, W., 355, 366, 367, 368, 369, 408, 411
 McKenney, J., 355, 356, 357, 378, 381, 408, 411
 McPhee, S., 119
 Media, network, 206, 208
 Media controls, 260, 265
 Medicaid: certification for, 62, 64; and history of health care information systems, 93, 95, 96, 97, 98, 100, 105; telemedicine reimbursement by, 142
 Medical errors: information management practices contributing to, 47, 106; IOM report on, 105, 106, 122, 124; reduced with computerized order entry system, 420; reduced with information technology use, 119–120. *See also* Patient safety
 Medical records: automated, 113. *See also* Electronic medical record (EMR) systems; Patient medical records
 Medical Records Institute (MRI): on factors influencing EMR adoption, 118; on health care documentation, 47, 48; on levels of computerization of health information, 112–117, 244
 Medicare: certification for, 62, 64; cost reports, 29, 30; evolution of reimbursement systems of, 93, 99–100, 101–102; and history of health care information systems, 93, 95, 96, 97, 98, 99–100, 101; telemedicine reimbursement by, 142
 Medication administration systems, overview of, 131–132
 Medication errors: defined, 124; medication administration systems to reduce, 131–132; reduced with computerized provider order entry (CPOE) systems, 126

Medication records, 9
 Meehan, W., III, 381–382
 Memorial Sloan-Kettering Cancer Center, 120
 Mendelson, D., 141
 Merchia, P., 119
 Metzger, J., 125, 175, 180
 Michelson, J., 147
 Microcomputers, 100–101, 104
 Microwave transmission, 208
 Middleton, B., 126
 Middleware, 192
 Miller, E., 126
 Miller, M., 119, 120
 Miller, R., 135, 169
 Minicomputers, 96–97, 99
 Minimum Data Set (MDS), 19, 21
 Mon, D., 243
 Monitors, computer, 221
 Monolithic architecture, 228, 231
 Moyer, C., 104
 Mui, C., 356
 myPHR, 8

N

National Alliance for Health Information Technology (NAHIT), 233, 243
 National Center for Health Statistics, UHDDS developed by, 19
 National Center for Healthcare Statistics, ICD-9-CM (International Classification of Diseases) published by, 21, 23–25
 National Committee for Quality Assurance (NCQA): accreditation by, 72–73; health plan report cards from, 35–37, 73; HEDIS developed by, 32–35; mission and vision of, 72; report cards on health plans approved by, 35–37
 National Committee on Vital and Health Statistics (NCVHS): ACDS approved by, 21; and National Healthcare Information Infrastructure (NHII), 247, 248; recommendations on standards for patient medical record information (PMRI), 237–238, 239
 National Council for Prescription Drug Programs (NCPDP), 242

National Electrical Manufacturers Association (NEMA), 241, 242
 National Healthcare Information Infrastructure (NHII), 247–248
 National Library of Medicine (NLM), Unified Medical Language System (UMLS), 238–239
 National Uniform Billing Committee (NUBC), 17
 National Uniform Claim Committee (NUCC), 17
 Natural language processing (NLP) programs, 217
 Net present value (NPV), 426, 428
 Network administrators, 291, 294
 Network interface cards (NICs), 205
 Network operating systems (NOSs), 204
 Networks, 200–209; communication devices in, 209; communication protocols for, 201–204; information processing distribution schemes for, 210; LAN vs. WAN, 205; media and bandwidth of, 206, 208–209; neural, 218; typologies of, 205–206, 207
 Neural networks, 218
 New projects, IT budget, 384
 Newman, J., 169
 North American Industry Classification System (NAICS), 452–453
 Notebook computers, 223, 224
 Nursing informatics officers, 151

O

Oates, R., 121
 Object-oriented database management systems (OODBMSs), 197
 Object-oriented databases (OODBs), 192, 197
 Object-oriented programming, 190–191
 Object-relational database management systems (ORDBMSs), 197
 Object-relational databases (ORDBs), 192
 Office of the National Coordinator for Health Information Technology, 248
 On-line transactional processing (OLTP) databases, 198–199
 Ongoing projects, IT budget, 384

Open Database Connectivity (ODBC) standard, 194
 Open Standards Interconnection (OSI) model, 201, 202–203
 Operating budgets, 306, 384
 Operating systems, 191, 234, 235; network (NOSs), 204
 Operative reports, 11
 Optical bar-code recognition devices, 219–220
 Optical disk technology, 222
 Optical tape, 222
 Orange Book (Department of Defense), 264
 Organizational change: strategies for managing, 393–396; types of, 391–393
 Organizational form or characteristics, competitive advantage from changing, 350–351
 Organizational performance, relationship between IT investments and, 444–445
 Organizational processes, leveraging, 346–348
 Organizational strategy: formulation of, 316–317; implementation of, 317–318; IT governance linked to, 364–366; IT investment for initiatives related to, 424–425; IT strategies linked to, 320, 439–440. *See also* IT strategy and alignment
 Ornstein, S., 119, 120, 169
 ORYX, 37–38
 Osborn, E., 119
 Outcomes: CPOE systems as improving, 127; electronic medical records (EMRs) as improving, 119–120; failure to manage, 442, 443
 Outcomes measures, 31–32
 Output devices, 221
 Overhage, J., 119, 120
 Oz, E., 191, 209, 211, 212, 213, 214, 215, 216, 218, 219, 220, 221, 222, 223, 225, 264, 270, 272, 274, 275, 300, 301

P

Packet filter firewalls, 275
 Palmetto Physicians Primary Care, 154–155

- Pan, E., 126
- Partners HealthCare, 296–297, 302–303
- Passino, J., 407
- Password systems, 270–271
- Pastore, R., 344
- Pathology reports, 11
- Patient care: continuity of, and
poor-quality documentation, 47;
as purpose of patient medical
records, 7
- Patient encounters: form for, show-
ing HCPCS/CPT codes for, 26;
for hospital admission, 12–14;
for office visit to physician,
15–16; types of data and infor-
mation from, 6
- Patient medical record information
(PMRI), standards for terminol-
ogy in, 237–239
- Patient medical records: authentica-
tion of, 74, 80–81; consequences
of poor-quality documentation
in, 45–47; content of, 8–12;
JCAHO standards for content
and maintenance of, 67, 69–72;
as legal documents, 75–79; pri-
vacy and confidentiality of,
81–85; problems with paper-
based, 112; purpose of, 7–8; re-
tention and destruction of,
79–80; from typical hospital ad-
missions, 12–14; from typical
physician's office visits, 15. *See also* Electronic medical record
(EMR) systems
- Patient safety: computerized
provider order entry (CPOE)
system as improving, 106, 124,
126, 420; electronic medical
records (EMRs) as improving,
119–120; Institute of Medicine
report on, 105–106; and poor-
quality documentation, 47, 106.
See also Medical errors
- Patient Safety* (Institute of Medicine),
105–106
- Patient-specific data and informa-
tion: administrative, 16–21,
22–23; clinical, 7–16; combin-
ing clinical and administrative,
21, 23–26. *See also* Patient med-
ical records
- Penrod, L., 121
- Periodicals, health care industry,
455–456
- Personal digital assistants (PDAs),
107, 225
- Pestonik, S., 119
- Physical. *See* History and physical
- Physical access controls, 259, 266
- Physical safeguards, 265–267; as-
signed security responsibility for,
265; HIPAA Security Rule stan-
dards on, 259–260; media con-
trols as, 260, 265; physical access
controls as, 259, 266; worksta-
tion security as, 260, 266–267
- Physicians: adoption of clinical in-
formation systems resisted by,
143–144; CPOE systems re-
sisted by, 179–180; evolution of
methods of reimbursing, 100,
101–102; patient medical
records generated from office
visits to, 15
- Physician's orders, 10, 14
- Piccione, R., 154–155
- Picture archival and communica-
tion systems (PACS), 421
- Pierson, S., 119
- PIN systems, 270–271
- Pineault, R., 121
- Plaintext, 273
- Planning, for managing change, 396.
See also IT planning; IT strategy and
alignment
- Platforms, information systems ar-
chitecture, 227
- Plug-ins, 212
- Poon, E., 143
- Porter, M., 324, 343
- Post Office Protocol 3 (POP3), 214
- Potvin, L., 121
- Precision of data, 53, 57
- Pretty Good Privacy (PGP), 273, 274
- Printers, computer, 221
- Privacy, 81–83; defined, 81; federal
laws on, 82–85; recent viola-
tions of, 82; and security, 251
- Privacy Act of 1974, 83
- Privacy Rule, HIPAA, 82–83, 84–85
- Problem lists, 9
- Problems, types of, 215
- Procedural programming lan-
guages, 190
- Productivity, and electronic medical
records (EMRs), 120
- Products: differentiation of, compet-
itive advantage gained with,
349–350; focus on inappropri-
ate aspects of, 442; new, IT in-
vestments for development of,
424
- Professional associations, 457–460
- Programmers, 289
- Programming languages, 190–191,
194
- Progress notes, 10, 14
- Project charters, 401, 461–472
- Project complexity, and failure of
IT initiatives, 410–411
- Project management, 396–407;
committees for, 399–400; man-
gled, and return on IT invest-
ments, 443; objectives of,
396–397; and project charter,
401, 461–472; and project plan,
402–405; and project status re-
port, 405–407; roles important
for, 397–399
- Project manager, responsibilities of,
398–399
- Project plans: and project manage-
ment, 402–405; for system im-
plementation, 171–177
- Project proposals: common prob-
lems in reviewing, 431–433; di-
versity of IT value from,
420–425; required for all IT
projects, 434; scoring, 336, 337,
427, 429; value portion of,
425–433. *See also* IT budgets
- Project repositories, system acquisi-
tion, 162–163
- Project review committee, 400
- Project status reports, 405–407
- Project steering committee: for proj-
ect management, 399–400; for
system acquisition, 150–151
- Project teams, 400
- Proposals, vendor, 159–161, 442.
See also Project proposals
- Protected health information (PHI),
4; ePHI, 256; under HIPAA,
84–85, 256
- Protocols: Hypertext Transfer Pro-
tocol (HTTP), 212, 213, 214;
Internet, 212, 214; network
communication, 201–204; vs.
standards, 201
- Proxy server firewalls, 275

Public Key Infrastructure (PKI), 272–274
 Public safety, and poor-quality documentation, 47
 Purohit, A., 131
 Purpose, clarity of, and IT initiative failure, 408

Q

Quality. *See* Health care data quality
 Quality Compass, 35, 72
 Quality improvement, IT investments for, 424
 Quality of care: improved with electronic medical records (EMRs), 119–120; monitored with patient medical records, 8
 Quinsley, C. A., 256

R

Radical change, 393
 Random data errors, 57, 58
 Raymond, B., 102, 119
 Recruitment and retention, IT staff, 296–297
 Redundant array of independent disks (RAID), 221–222
 Reengineering process, 173
 Registers, specialized, 27–28
 Reimbursement: as barrier to adopting clinical information systems, 141–143; capitated, 100; cost-based, 93; DRG-based system for, 99–100; fee-for-service, 100; forms for processing claims for, 16–17, 18–19, 20; resource-based relative values scale (RBRVS), 101–102; for telemedicine, 105, 134, 142–143. *See also* Billing
 Relational database management systems (RDBMSs), 193–194
 Relational databases (RDBs), 192–197; database management systems for, 193–194; and relational data modeling, 194–197
 Release of information, 85–88
 Relevance of data, 53, 57
 Remondin, M., 121
 Renner, K., 120
 Repeaters, 209

Report cards: from HealthGrades, 40; on NCQA-approved health plans, 35–37, 73
 Report generation, 47
 Request for information (RFI), system acquisition, 156–157
 Request for proposal (RFP), system acquisition, 154, 155–156, 157, 159–160, 161, 165
 Required specifications, HIPAA Security Rule, 257
 Research, as purpose for patient medical records, 8
 Research firms, health care IT industry, 457
 Resistance, user, to system implementation, 143–144, 179–181
 Resource-based relative value scale (RBRVS) reimbursement, 101–102
 Resources: allocating, in system implementation, 181–182; limited, and failure of IT initiatives, 411–412
 Retention: of IT staff, 296–297; of patient medical records, 79–80
 Return on investment (ROI), 424, 440–441
 Reward system, and failure of IT initiatives, 410
 Reynolds, G., 197, 200, 201, 204, 209, 211, 212, 213, 215, 217, 219, 222
 Ridsdale, L., 121
 Ring typology, 205, 206
 Risk analysis, 258, 262–263
 Risk management, 258, 263
 Rob, P., 192
 Roberge, D., 121
 Rodnick, J., 119
 Role-based access control (RBAC), 268
 Ross, J., 354, 363, 374, 377, 422
 Routers, network, 209
 Rust, P., 119
 RxNorm, 239
 Rybak, M., 119

S

Safran, C., 120
 Sambamurthy, V., 309, 312, 373, 375

Satisfaction: with CPOE systems, 127; improved with electronic medical records (EMRs), 120–121
 Scheffer, G., 57–58
 Schmitz, J., 119
 Schneider, J., 235
 Schott, S., 45, 46, 60
 Scoring, project proposals, 336, 337, 427, 429
 Scottsdale Institute, 459
 Second generation languages, 190
 Security, 250–277; administrative safeguards of, 257–259, 261–265; general aspects of, 251–252; physical safeguards of, 259–260, 265–267; standards for, 257–261, 264–265; technical safeguards of, 260–261, 267–276; threats to, 252–255; with wireless technologies, 276–277. *See also* Security Rule, HIPAA
 Security officers, 258, 263–264
 Security Rule, HIPAA: overview of, 256–257; standards of, 257–261
 Sentinel events, 66
 Service carriers, network, 208
 Services: competitive advantage with differentiation of, 349–350; improved with electronic medical records (EMRs), 120–121; new, IT investments for development of, 424
 Severance, D., 407
 Shakir, A., 56
 Shared computing systems, 96
 Short, J., 173
 Signatures, electronic, 80–81
 Sim, I., 169
 Simon, H., 215
 Simple Mail Transfer Protocol (SMTP), 214
 Singer, S., 104
 Sittig, D., 129
 Slack, W., 120
 Slomovic, A., 235
 Smart phones, 225
 Smith, H., 268
 SNOMED International, 237, 238
 Software: antivirus, 275–276; and interface engines, 191–192, 193; middleware, 192; programming

- languages used in, 190–191; system, 190–191; terminal emulation, 210; types of, 190
 - Solomon, G., 121
 - Source data input devices, 219–220
 - Sousa, K., 134
 - Speech output, 221
 - Speech recognition, 220
 - Spread spectrum radio transmission, 208
 - Spurr, C., 119, 397
 - Staff: saving fractions of effort by, 431; training, for system implementation, 174–176, 182–183. *See also* IT staff
 - Stair, R., 197, 200, 201, 204, 209, 211, 212, 213, 215, 217, 219, 222
 - Standards, 233–249; as barrier to adopting clinical information systems, 144; for coding, 25; for data interchange and integration, 239–243; development of, 234–236; for health record content, 243–245; in HIPAA Security Rule, 257–261; impact of HIPAA on, 234, 246–247; IT, 233–234, 235, 264–265; vs. protocols, 201; for wireless networks, 204, 276. *See also specific standards*
 - Standards development organizations (SDOs), ANSI-accredited, 235, 236
 - Star typology, 206, 207
 - State laws, 74–75
 - Stavri, P., 169
 - Stead, W., 120, 129
 - Steck, J., 120
 - Stein, D., 131
 - Step-shift change, 392–393, 394
 - Stern, D., 104
 - Stoddard, D., 368
 - Store and forward technology, telemedicine programs, 133
 - Straisor, D., 362
 - Strassman, P., 444
 - Strategic planning. *See* IT planning; IT strategy and alignment
 - Strategic trajectories, IT strategies based on, 322–323
 - Strategy. *See* IT strategy and alignment; Organizational strategy
 - Structured query language (SQL), 190, 194, 233, 234
 - Stuntz, L., 420
 - Superior Consultant Company, 160
 - Support: following system implementation, 183; as function of IT department, 283; for integrated delivery system (IDS), 364–365; in IT budget, 384; leadership, and failure of IT initiatives, 408–409
 - Support systems, for decision making, 215–218, 323
 - Switches, network, 209
 - System acquisition, 146–166; common problems in, 164–165; communication in, 163; cost-benefit analysis in, 161–162; defined, 147; evaluating, 306; evaluating vendor proposals in, 159–161, 442; example of, 148–150; exploring contracting options in, 157–159; goals in, 151–152, 153; identifying system requirements in, 153–155; negotiating with vendors in, 162, 165; prerequisite for, 147; project management tools used in, 162–164; project steering committee for, 150–151; request for information (RFI) in, 156–157; request for proposal (RFP) in, 154, 155–156, 157, 159–160, 161, 165; researching products and vendors in, 152–153; steps in, 149; summary report and recommendations in, 162
 - System analysts, 288–289
 - System champion, system implementation, 169
 - System implementation, 167–185; allocating resources for, 181–182; checklist for, 415–416; common problems in, 177–183; communicating progress in, 176–177; data conversion in, 176; defined, 168; evaluating, 307; go-live date in, 177; goals and expectations of, 170–171, 178–179; implementation team for, 168–169; installation of system components in, 174; managing organizational change accompanying, 391–396; project plan for, 171–177; recommendations for, 414–415; shortened cycle of deliverables in, 437; staff training in, 174–176, 182–183; system champion for, 169; user resistance in, 179–181; workflow analysis in, 172–174
 - System maintenance and support, 183
 - System software, 190–191
 - Systematic data errors, 57, 58
 - Systematized Nomenclature of Medicine—Clinical Terms (SNOMED CT), 237–238
 - Systems programmers, 289
- ## T
- T-1 lines, 208
 - Tablet computers, 223, 224
 - Tape drives, 221
 - Targets, budget, 385
 - Tate, K., 120
 - Taylor, H., 135
 - Technical safeguards, 267–276; access control as, 260, 267–269; audit trails as, 272; data encryption as, 260, 261, 272–274, 276; entity authentication as, 261, 269–272; firewalls as, 274–275; HIPAA Security Rule standards on, 260–261; virus checking as, 275–276
 - Technology. *See* Information technology (IT)
 - Teich, J., 119, 124, 129, 130
 - Telecommunications carriers, 208
 - Telecommunications specialists, 294
 - Telehealth, 104, 132, 134–137. *See also* Electronic mail (e-mail)
 - Telemedicine, 132–134; benefits of, 134; current programs for, 132–133; defined, 104–105, 132; methods of delivering, 133; reimbursement for, 105, 134, 142–143; vs. telehealth, 132
 - Telephones: Internet telephoning, 214; smart phones, 225; telephone callback procedures, 271–272
 - Telesurgery, 133

Terasawa, E., 118, 125
 Terminal emulation software, 210
 Terminal-to-host distribution schemes, 210
 Terminology: information systems architecture, 227; information systems (ISs), 92; standards for patient medical record information (PMRI), 237–239
 Thin client schemes, 210
 Third generation languages, 190
 Thumb drives, 222, 223
 Tierney, W., 119, 120
 Timelines: in project charter, 469; for proposed projects, 336, 338
 Timeliness of data, 54, 57
To Err Is Human (Institute of Medicine), 105, 106
 Tokens, 272
 Toole, J., 415
 Top-level domains (TLDs), 213, 214
 Torvald, L., 191
 Touch screens, 218–219
 Trackballs, 218
 Trackpads, 218
 Training: health care information systems damaged by lack of, 253–254; just-in-time, 175–176; strategy for, in project charter, 471–472; for system implementation, 174–176, 182–183
 Transmission Control Protocol/Internet Protocol (TCP/IP), 201
 Trigger events, HL7-defined, 240
 Trojan horses, 252–253, 275
 Trust, and managing organizational change, 395
Trusted Computer System Evaluation Criteria (TCSEC, Department of Defense), 264
 Turisco, F., 125
 Turnkey systems, 99
 Twisted pair wire, 208
 Two-way interactive television (IATV) technology, telemedicine programs, 133

U

UB-92, 17, 18–19
 Uncertainty, and failure of IT initiatives, 411

Unified Medical Language System (UMLS), 238–239
 Uniform Ambulatory Care Data Set (ACDS), 19, 21
 Uniform data sets, 16–21, 22–23
 Uniform Hospital Discharge Data Set (UHDDS), 17, 19, 21, 22–23
 Uniform resource locators (URLs), 212, 213, 214
 Unique identifiers, 260, 269
 University HealthSystem Consortium, 459
 University of Kansas Medical Center, telemedicine program, 132–133
 University of Texas Medical Branch (UTMB), telemedicine program, 133
 User-based access, 268
 Users: governance responsibilities of, 367; resistant to system implementation, 143–144, 179–181

V

Value. *See* IT value
 Van Hentenryck, K., 240
 Vectors: for arriving at IT strategy, 318–325; defined, 319
 Vendors: evaluating proposals of, 159–161, 442; major, in health care IT industry, 454–455; negotiating with, 162, 165; researching, 152–153
 Venkatraman, N., 315
 Viruses, computer, 252–253, 275–276
 Visionary applications, 375–376
 Visual integration architecture, 228, 231
 Visual programming, 190
 Voice over Internet Protocol (VoIP), 214
 Voice recognition, 107–108, 220
 Voluntary Hospitals of America, 459

W

Waegemann, C., 112
 Wager, K., 120, 121, 144, 169
 Wagner, T. H., 104
 Wahl, R., 147
 Walker, J., 126

Walsh, T., 262, 264, 270
 Wang, S., 120, 420
 Ward, D., 120, 169
 Weaver, L., 120
 Web browsers, 212
 Web developers, 295
 Web masters, 294–295
 Web-site development and maintenance, outsourcing, 304
 Webopedia, 205, 272
 Weil, S., 262
 Weill, P., 339, 363, 374, 377, 379, 444
 Weingarten, S., 119
 Whatis?com, 194, 201, 204, 208, 209, 211, 212, 213, 214, 270, 271, 274, 275
 Wheeler, L., 134
 White, A., 120, 169
 White, C., 201, 208, 270, 271, 273, 274, 275, 276
 Whitten, J., 92, 173
 Wi-Fi (802.11) standard, 204, 208
 Wide area networks (WANs), 205
 Wired Equivalent Privacy (WEP), 276
 Wireless technologies, 107, 276–277, 335
 Wise, P., 243
 Workflow analysis, system implementation plan, 172–174
 Workstation security, 260, 266–267
 World Health Organization, International Classification of Diseases, 21, 25
 World Wide Web (WWW), 212–213
 Worms, 252–253, 275

X

X-ray reports, 10

Y

Yarnall, K., 119

Z

Zaran, F., 119
 Zhou, X., 119
 Zimmermann, P., 274
 Zmud, R., 375