CompTIA® Healthcare
IT Technician HIT-001
Authorized Cert Guide

Joy Dark
Jean Andrews, Ph.D.
CompTIA® Healthcare IT Technician HIT-001 Authorized Cert Guide

Copyright © 2012 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and authors assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-10: 0-7897-4929-7

The Library of Congress Cataloging-in-Publication data is on file.

Printed in the United States of America

Second Printing: July 2012

Trademark

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Bulk Sales

Pearson IT Certification offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearson.com

Associate Publisher
David Dusthimer
Acquisitions Editor
Betsy Brown
Senior Development Editor
Christopher Cleveland
Managing Editor
Sandra Schroeder
Project Editor
Mandie Frank
Copy Editor
Apostrophe Editing Services
Indexer
Brad Herriman
Proofreader
Paula Lowell
Technical Editors
Chris Crayton, Isaias Leiva, Steve Picray, Ken Toth
Publishing Coordinator
Vanessa Evans
Multimedia Developer
Tim Warner
Book Designer
Gary Adair
Cover Designer
Sandra Schroeder
Composition
Bronkella Publishing
# Contents at a Glance

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>xxxix</td>
</tr>
<tr>
<td>CHAPTER 1: Introducing Healthcare IT</td>
<td>2</td>
</tr>
<tr>
<td>CHAPTER 2: Introducing Data Flow in HIT</td>
<td>24</td>
</tr>
<tr>
<td>CHAPTER 3: Regulatory Requirements</td>
<td>64</td>
</tr>
<tr>
<td>CHAPTER 4: Organizational Behavior</td>
<td>96</td>
</tr>
<tr>
<td>CHAPTER 5: IT Operations</td>
<td>148</td>
</tr>
<tr>
<td>CHAPTER 6: Medical Business Operations</td>
<td>226</td>
</tr>
<tr>
<td>CHAPTER 7: Security</td>
<td>280</td>
</tr>
<tr>
<td>APPENDIX A: Answers to Acronym Drills, Review Questions, and Practical Application Exercises</td>
<td>320</td>
</tr>
<tr>
<td>APPENDIX B: CompTIA Healthcare IT Technician ACRONYMS</td>
<td>336</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Terms Glossary</td>
<td>342</td>
</tr>
<tr>
<td>Index</td>
<td>358</td>
</tr>
</tbody>
</table>
# Table of Contents

## Introduction  xxxix

### Chapter 1  Introducing Healthcare IT  2

- The Importance of the HITECH Act  3
- Getting to Know Healthcare  5
  - Types of Healthcare Facilities  6
  - Focus on Hospitals  7
  - Departments in the Hospital  8
- Patient Flow Through a Hospital Stay  9
  - *Inpatient Admittance*  9
  - *Outpatient Admittance*  11
  - *Emergency Department Patient*  12
- The Goals of Healthcare IT  15
  - Why Have IT in Healthcare?  15
  - Prepare for a Career in Healthcare IT  16

### Chapter Summary  19

- *The Importance of the HITECH Act*  19
- *Getting to Know Healthcare*  19
- *Goals of Healthcare IT*  20

### Key Terms  20

### Acronym Drill  21

### Review Questions  22

### Practical Application  23

## Chapter 2  Introducing Data Flow in HIT  24

- Learning Support Flow  25
- Getting to Know Information Systems  27
- Getting to Know HIS  28
  - Functions of an HIS  29
- Getting to Know the Interface  33
  - The Message  34
  - The Message Path  36
Chapter 3 Regulatory Requirements 64
Identifying Standard Agencies, Laws, and Regulations 65
  Agencies Governing Healthcare 65
  Department of Health and Human Services 66
  National Institute of Standards and Technology (NIST) 72
Healthcare Programs 74
Healthcare Laws 76
  Health Insurance Portability and Accountability Act (HIPAA) 76
  American Recovery and Reinvestment Act (ARRA) 77
  Health Information Technology for Economic and Clinical Health (HITECH) Act 78
Regulations of Healthcare Laws 79
Learning HIPAA Controls and Compliance Issues 80
Learning Rules of Record Retention and Disposal 83
Types of Health Records 83
Record Retention 85
Record Disposal 85

Learning Legal Best Practices and Documentation 86

Chapter Summary 90
Identifying Standard Agencies, Laws, and Regulations 90
Learning HIPAA Controls and Compliance Issues 91
Learning Rules of Record Retention and Disposal 91
Learning Legal Best Practices and Documentation 92

Key Terms 92
Acronym Drill 93
Review Questions 93
Practical Application 94

Chapter 4  Organizational Behavior 96

Handling PHI 97
Physical Safeguards 98
Technical Safeguards 103

Applying Proper Communication Methods 105
E-Mail 106
IM Versus Secure Chat 106
EMR/EHR System 107
Fax 108
Secure FTP 108
Phone 109
VoIP 111

Identifying EHR/EMR Access Roles and Responsibilities 113
Medical and Medical Support Roles 114
Technical Roles 119
System Administrator 119
Security Administrator 120
Network Administrator 121
Database Administrator 122
Desktop Support Technician 123
Third-Party Access 123
Role-Based Access and Exceptions 124
Access Based on Sensitive Patient Data 126
Levels of Access and Audit Trails 126
Identifying Organizational Structures and Different Methods of Operation 127
Hospitals 127
Private Practices 129
Nursing Homes 130
Assisted Living Facilities 130
Surgical Centers 131
Home Healthcare 131
Hospice 131
Executing Daily Activities 132
Communication 132
IT Functions in a Healthcare Environment 133
HIT Technician Presence in the Hospital 134
Chapter Summary 139
Handling PHI 139
Applying Proper Communication Methods 139
Identifying EHR/EMR Access Roles and Responsibilities 139
Identifying Organizational Structures and Different Methods of Operation 141
Executing Daily Activities 141
Key Terms 142
Acronym Drill 144
Review Questions 144
Practical Application 146

Chapter 5 IT Operations 148
How the Internet or an Intranet Works 149
The OSI Model 151
Application, Presentation, and Session Layer Protocols 153
Transport and Network Layers 156
Data Link and Physical Layers 159
Servers on the Network 160
Cloud Computing and Virtualization 163
Programming Languages 168

How a Network Works 172
Basic Network Devices and Hardware 175
Wireless Access Point 175
Router 177
Switch 182
Internet Modem 183
Network Tools 184
ipconfig Command 184
ping Command 185
tracert Command 186
Solving Network Problems 188
Duplicate IP Address 189
Broken Cables and Crosstalk 190
Interference with Wireless Networks 190
Poor AP Placement 190
Lost Connectivity to the ISP 191
Power Failure, Blackouts, and Brownouts 191

Managing Network Resources 192
Locally Hosted or Remote EHR and EMR Information Systems 193
Considerations for Servers on a Network 194
Security Risks 195
High Traffic and Load Balancing 196
Hardware and Software Specifications Required by Vendors 196
Purging Old Logs 196
Maintain Backups and Downtime Procedures 196

Configuring a Workstation and Peripherals 198
Deploy a Workstation 198
Maintain Operating System Updates 203
Troubleshoot Common Problems 204
Problems with a Mouse 204
Problems with a Monitor 205
Problems with a Printer 205
Power Problems 206
Software Patches, Hotfixes, and Updates 206
Peripheral Devices 207
Mobile Storage 211
Flash Drives and External Hard Drives 211
DVDs and CDs 212
SD Cards 212
Tapes 212
Mobile Computing Devices 213
Chapter Summary 215
How the Internet or an Intranet Works 215
How a Network Works 215
Managing Network Resources 216
Configuring a Workstation and Peripherals 216
Key Terms 217
Acronym Drill 219
Review Questions 220
Practical Application 224

Chapter 6  Medical Business Operations 226
Understanding the Clinical Environment 227
Medical Terms, Imaging, and Tests 228
Medical Terms 228
Medical Imaging 232
Medical Tests 236
Medical Departments 240
Clinical Environment 242
Supporting Software Used in Healthcare Facilities 245
Clinical Software and Modules 246
Scheduling Software 246
Patient Tracking Software 247
Order Entry Software 248
Practice Management Software 249
Billing and Coding Software 250
Tracking and Auditing Software 252
Document Imaging 253
Medical Images of the Human Body 253
Digital Images of Patient Records 255
Change Control 256
Support Requests 258
How a Healthcare Interface Works 259
HL7 Message 260
Typical Interface Issues 262
Chapter Summary 266
Understanding the Clinical Environment 266
Supporting Software Used in Healthcare Facilities 267
How a Healthcare Interface Works 269
Key Terms 270
Acronym Drill 271
Review Questions 272
Practical Application 275

Chapter 7  Security 280
What Are We Up Against? 281
Social Engineering 281
Electronic Attacks 282
Understanding Permission Levels 283
Understanding Physical Security 285
Location and Access 286
Servers 286
Network Hardware 287
Printers, Scanners, and Copiers 289
Accessing Secured Resources 290
Environmental Security 293
Using Password Best Practices 294
Understanding Encryption Types 296
Types of Encryption 296
Communication 298
About the Authors

Joy Dark has worked in the healthcare IT field in several capacities. She first worked as a help desk technician providing first-level support at a company that supports more than 130 hospitals in 29 states. Later she focused on providing second-level support for clinical information systems, specializing in perioperative information systems and the emergency department information systems. Next she switched gears to become a support operations specialist, helping to design support protocols and structures as well as managing the transition of support when hospitals converted information systems. Now she has authored the CompTIA Healthcare IT Technician HIT-001 Cert Guide and contributes in writing other technical books. Before healthcare IT, Joy was an elementary school teacher in both the United States and in South America. She lives in Dalton, Georgia, with her sister and Doberman dog. She has two sisters who are physicians (anesthesiology and emergency medicine) who have shared plenty of stories, facts, and opinions about the healthcare environment that have helped to shape the content in this book.

Jean Andrews, Ph.D., has more than 30 years of experience in the computer industry, including more than 13 years in the college classroom. She has worked in a wide variety of businesses and corporations designing, writing, and supporting applications software; managing a PC repair help desk; and troubleshooting wide area networks. She has written a variety of books on software, hardware, and the Internet. She lives in northeast Georgia.

About the Reviewers

Chris Crayton is an author, technical editor, technical consultant, and trainer. Formerly, he worked as a computer and networking instructor at Keiser University; as network administrator for Protocol, a global electronic customer relationship management (eCRM) company; and at Eastman Kodak Headquarters as a computer and network specialist. Chris has authored several print and online books on PC Repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. Mr. Crayton has also served as technical editor and contributor on numerous technical titles for many of the leading publishing companies. He holds MCSE, A+, and Network+ certifications.
**Isaias Leiva** is a professor at city college of San Francisco where he teaches computer networking and information technology topics. He is also a technical training manager at the stride center, a very successful non-profit organization where he develops curriculum and manages the training program that prepares students for industry certifications. Professor Leiva has also written and implemented a set of life skills and professional skills that prepare students for the work place. He has also contributed very valuable training videos through his YouTube channel which has gained worldwide audience. He is A+, Network+, IC3, MOS, MCP, MCDST certified and holds an AS in CNIT from CCSF.

**Steven M. Picray** is a medical surgical registered nurse in a major metropolitan hospital. He has also been a Baptist pastor and a computer programmer. He has bachelor’s and master’s degrees in Theology, and is a few months away from obtaining his BSN in preparation for advanced practice nursing.

**Kenneth J. Toth** is a Business and Information Technology instructor who has worked at Coloma Community Schools (1989–1998), Careerline Tech Center (1999–present), and Lake Michigan College (2110–present). He holds Certiport IC3 GS3, ETA CSS, Oracle Data Modeling/SQL/Java, CompTIA A+, Network+, Security+, and Healthcare IT certifications. Ken serves on the CompTIA Education Advisory Council and he is an active member of the Marketing, Attendance, and Scholarship committees at Careerline Tech Center.
Dedication

This book is dedicated to the covenant of God with man on earth.
Acknowledgments

Being my first book, I have a lot of people to thank for helping me. Without their support and mentorship, this book might never have happened.

First, I would like to thank Pearson for giving the book and me this opportunity. David Dusthimer took a leap of faith in me and believed in the potential of this book. Betsy Brown encouraged me as a new author with a little hand-holding when deadlines seemed overwhelming. Chris Cleveland guided this project and provided helpful feedback. The reviewers have been fantastic and have helped to polish this book: Chris Crayton, Steve Pickray, Ken Toth, and Isaias Leiva. The researchers who contributed to this book: Bambi Cannon, Casey Jo Baldridge, Shelia Howard, Pam Ownby, and Jill West (photo research), raised this book to the next level of quality with the information they each provided. I also acknowledge various people who have also contributed to the success of this book: Sandra Schroeder, Vanessa Evans, Tim Warner, and Gary Adair.

Finally, I acknowledge my mother, Jean Andrews. She has been my mentor and support through the entire writing process. She has been there in moments of stress, helping me figure out how to fix things, and in moments of celebration, helping me to rejoice in the victories to encourage me to keep going.

—Joy Dark

Would “I’m a proud mama!” be appropriate to say here? When Joy and I took on this daughter/mother mentoring arrangement, we both had hopes this would work, but actually my expectations have been greatly exceeded. It’s been fun! Joy, I’m proud of you! Way to go!

—Jean Andrews
We Want to Hear from You!

As the reader of this book, you are our most important critic and commentator. We value your opinion and want to know what we’re doing right, what we could do better, what areas you’d like to see us publish in, and any other words of wisdom you’re willing to pass our way.

As an associate publisher for Pearson IT Certification, I welcome your comments. You can e-mail or write me directly to let me know what you did or didn’t like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book’s title and author as well as your name, e-mail address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com
Mail: David Dusthimer
Associate Publisher
800 East 96th Street
Indianapolis, IN 46240 USA
CompTIA Healthcare IT Technician

The CompTIA Healthcare Technician specialty certification is a vendor and technology neutral exam designed to ensure IT professionals have the operational, regulatory and security knowledge necessary to provide hardware and software support in medical environments where Electronic Health Record systems are being deployed or maintained.

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill—Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation and promotion.

Ten of the twenty fastest growing occupations in the US are healthcare-related, potentially yielding 3.2 million new jobs over the next decade.

- **U.S. HITECH ACT**—Funded imperative for US healthcare industry
- **Transition paper records**—In U.S medical facilities by year-end 2015
- **Individual physicians receive $40K+**—Installing EHRs and demonstrating “meaningful use.”
- **More than $88.6 billion**—Spent by providers in 2010 on developing and implementing EHRs, health information exchanges (HIEs) and other HIT initiatives, HIT and consulting vendors expected to see a 10% to 20% hike in revenues in 2012
Healthcare IT: A Growing Opportunity

U.S. officials estimate healthcare IT jobs will grow by at least 50,000 between February 2010 and February 2015. That’s more than 12,000 new jobs per year.

Healthcare IT jobs are growing everywhere.

The average base salary for a Healthcare IT tech is $78,000.

How Certification Helps Your Career

- **IT Is Everywhere**
  - IT is ubiquitous, needed by most organizations. Globally, there are over 600,000 IT job openings.

- **IT Knowledge and Skills Gets Jobs**
  - Certifications are essential credentials that qualify you for jobs, increased compensation, and promotion.

- **Retain Your Job and Salary**
  - Make your expertise stand above the rest. Competence is usually retained during times of change.

- **Want to Change Jobs**
  - Certifications qualify you for new opportunities, whether locked into a current job, see limited advancement, or need to change careers.

- **Stick Out from the Resume Pile**
  - Hiring managers can demand the strongest skill set.
CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.

POTENTIAL CAREER PATH

HEALTHCARE IT SPECIALIST

CERTIFICATE

PC REPAIR AND SUPPORT

CERTIFICATION

HEALTHCARE IT TECHNICIAN™

CERTIFICATE

A+®
### Steps to Getting Certified and Staying Certified

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Exam Objectives</td>
<td>Review the certification objectives to make sure you know what is covered in the exam: <a href="http://certification.comptia.org/Training/testingcenters/examobjectives.aspx">http://certification.comptia.org/Training/testingcenters/examobjectives.aspx</a></td>
</tr>
<tr>
<td>Practice for the Exam</td>
<td>After you have studied for the certification, take a free assessment and sample test to get an idea of what type of questions might be on the exam: <a href="http://certification.comptia.org/Training/testingcenters/samplequestions.aspx">http://certification.comptia.org/Training/testingcenters/samplequestions.aspx</a></td>
</tr>
<tr>
<td>Purchase an Exam Voucher</td>
<td>Purchase your exam voucher on the CompTIA Marketplace, which is located at: <a href="http://www.comptiastore.com/">http://www.comptiastore.com/</a></td>
</tr>
<tr>
<td>Take the Test!</td>
<td>Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: <a href="http://certification.comptia.org/Training/testingcenters.aspx">http://certification.comptia.org/Training/testingcenters.aspx</a></td>
</tr>
</tbody>
</table>

### Join the Professional Community

<table>
<thead>
<tr>
<th>Join IT Pro Community</th>
<th><a href="http://itpro.comptia.org">http://itpro.comptia.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The free IT Pro online community provides valuable content to students and professionals</td>
</tr>
<tr>
<td></td>
<td>Career IT Job Resources</td>
</tr>
<tr>
<td></td>
<td>■ Where to start in IT</td>
</tr>
<tr>
<td></td>
<td>■ Career Assessments</td>
</tr>
<tr>
<td></td>
<td>■ Salary Trends</td>
</tr>
<tr>
<td></td>
<td>■ US Job Board</td>
</tr>
<tr>
<td></td>
<td>Forums on Networking, Security, Computing and Cutting Edge Technologies</td>
</tr>
<tr>
<td></td>
<td>Access to blogs written by Industry Experts</td>
</tr>
<tr>
<td></td>
<td>Current information on Cutting Edge Technologies</td>
</tr>
<tr>
<td></td>
<td>Access to various industry resource links and articles related to IT and IT careers</td>
</tr>
</tbody>
</table>
Content Seal of Quality

This courseware bears the seal of CompTIA Approved Quality Content. This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

Why CompTIA?

- **Global Recognition**—CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA’s certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.

- **Valued by Hiring Managers**—Hiring managers value CompTIA certification, because it is vendor- and technology-independent validation of your technical skills.

- **Recommended or Required by Government and Businesses**—Many government organizations and corporations either recommend or require technical staff to be CompTIA certified. (For example, Dell, Sharp, Ricoh, the U.S. Department of Defense, and many more.)

- **Three CompTIA Certifications ranked in the top 10**—In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to obtain more information

- **Visit CompTIA online**—www.comptia.org to learn more about getting CompTIA certified.

- **Contact CompTIA**—Call 866-835-8020 ext. 5 or email questions@comptia.org.

- **Join the IT Pro Community**—http://itpro.comptia.org to join the IT community to get relevant career information.

- **Connect with us**—LinkedIn, Facebook, Twitter, Instagram, YouTube.
<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Regulatory Requirements</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>1.1 Identify standard agencies, laws, and regulations.</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- HHS</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- ONC</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- CMS</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- HIPAA</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- Medicare</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- Medicaid</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- ARRA</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- HITECH</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- Meaningful use</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- Eligible provider</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>- NIST</td>
<td>3</td>
<td>65-80</td>
</tr>
<tr>
<td>1.2 Explain and classify HIPAA controls and compliance issues.</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>- PHI</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>- Covered Entity</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>- Security</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>- HIPAA Security</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>- Violations</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>- Fines</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>- Requirements</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>- Release of information</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>- Access permissions</td>
<td>3</td>
<td>80-82</td>
</tr>
<tr>
<td>1.3 Summarize regulatory rules of record retention, disposal, and archiving.</td>
<td>3</td>
<td>83-86</td>
</tr>
<tr>
<td>- Documentation requirements</td>
<td>3</td>
<td>83-86</td>
</tr>
<tr>
<td>- Time of storage</td>
<td>3</td>
<td>83-86</td>
</tr>
<tr>
<td>- Types of records</td>
<td>3</td>
<td>83-86</td>
</tr>
<tr>
<td>- Public records</td>
<td>3</td>
<td>83-86</td>
</tr>
<tr>
<td>- Private records</td>
<td>3</td>
<td>83-86</td>
</tr>
<tr>
<td>- Legal health record</td>
<td>3</td>
<td>83-86</td>
</tr>
<tr>
<td>- Methods of record disposal</td>
<td>3</td>
<td>83-86</td>
</tr>
</tbody>
</table>
### Objective Chapter Pages

<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4 Explain and interpret legal best practices, requirements, and</td>
<td>3</td>
<td>86-88</td>
</tr>
<tr>
<td>documentation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Waivers of liability</td>
<td>3</td>
<td>86-88</td>
</tr>
<tr>
<td>■ Business Associate Agreements (BAA)</td>
<td>3</td>
<td>86-88</td>
</tr>
<tr>
<td>■ Third party vendor review and agreements (SLA, MOU)</td>
<td>3</td>
<td>86-88</td>
</tr>
<tr>
<td>2.0 Organizational Behavior</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2.1 Use best practices for handling PHI in the workplace.</td>
<td>4</td>
<td>97-105</td>
</tr>
<tr>
<td>■ PC placement</td>
<td>4</td>
<td>97-105</td>
</tr>
<tr>
<td>■ Privacy screens</td>
<td>4</td>
<td>97-105</td>
</tr>
<tr>
<td>■ Printer placement</td>
<td>4</td>
<td>97-105</td>
</tr>
<tr>
<td>■ Screensavers</td>
<td>4</td>
<td>97-105</td>
</tr>
<tr>
<td>■ Time lockout</td>
<td>4</td>
<td>97-105</td>
</tr>
<tr>
<td>2.2 Identify EHR/EMR access roles and responsibilities.</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Medical roles</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ MD</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ RN</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ PA</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ DA</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ PCT</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ MA</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ NUC</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ UA</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ LPN</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ PM</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Office Mgr.</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Staff</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Technical roles</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Security administrator</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Network administrator</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ System administrator</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>Objective</td>
<td>Chapter</td>
<td>Pages</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>■ Desktop support</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Database administrator</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Business Associate Access and Contractor Access</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Access limitations based on role and exceptions</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Emergency access (break the glass)</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Access based on sensitive patient data</td>
<td>4</td>
<td>113-127</td>
</tr>
<tr>
<td>■ Sensitivity labels and clearance</td>
<td>4</td>
<td>113-127</td>
</tr>
</tbody>
</table>

2.3 Apply proper communication methods in the workplace.

| ■ Email                                                                   | 4       | 105-112     |
| ■ IM vs. secure chat                                                      | 4       | 105-112     |
| ■ EMR system                                                              | 4       | 105-112     |
| ■ Fax                                                                     | 4       | 105-112     |
| ■ Secure FTP                                                              | 4       | 105-112     |
| ■ Phone                                                                   | 4       | 105-112     |
| ■ VoIP                                                                    | 4       | 105-112     |

2.4 Identify organizational structures and different methods of operation.

<p>| ■ Organizational Structures:                                             | 4       | 127-132     |
| ■ Hospital                                                               | 4       | 127-132     |
| ■ Private practice                                                       | 4       | 127-132     |
| ■ Nursing homes                                                           | 4       | 127-132     |
| ■ Assisted living facilities                                             | 4       | 127-132     |
| ■ Home healthcare                                                         | 4       | 127-132     |
| ■ Hospice                                                                | 4       | 127-132     |
| ■ Surgical centers                                                       | 4       | 127-132     |
| ■ Methods:                                                                | 4       | 127-132     |
| ■ Differences in scope of work                                           | 4       | 127-132     |
| ■ Availability of resources                                              | 4       | 127-132     |
| ■ Formality of procedures                                                | 4       | 127-132     |</p>
<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5 Given a scenario, execute daily activities while following a code of conduct.</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Communicate in a professional fashion</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Adapt procedural behavior according to different situations and environments</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Imaging room</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Procedural room</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Recovery room</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Examination room</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Float room</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Emergency room</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Adapt social behavior based on sensitivity of the environment</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Use proper sanitation steps—follow medical precautionary guidelines</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>■ Conform to requirements set forth by project manager</td>
<td>4</td>
<td>132-137</td>
</tr>
<tr>
<td>3.0 IT Operations</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>3.1 Identify commonly used IT terms and technologies.</td>
<td>5</td>
<td>149-192</td>
</tr>
<tr>
<td>■ Protocol terms:</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ TCP/IP</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ DNS</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ DHCP</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ FTP</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ Wireless (802.11x)</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ RDP</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ Devices:</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ Switch</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Domain controller</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ Printer server</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ Industry terms:</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ ASP</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ ISP</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>■ Client-server model</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>Objective</td>
<td>Chapter</td>
<td>Pages</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Mainframe</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>Cloud Computing</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>Virtualization</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>Terminal services</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>APIs</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>Fiber</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>Languages:</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>XML</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>SQL</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>HTML</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>Flash</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>PHP</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>ASP</td>
<td>5</td>
<td>149-172</td>
</tr>
<tr>
<td>3.2 Demonstrate the ability to setup a basic PC workstation within an EHR/EMR environment.</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Basic installation, configuration and maintenance procedures</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Basics of operating systems, mouse, keyboard, monitor and applications</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>3.3 Given a scenario, troubleshoot and solve common PC problems.</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Malfunctioning hardware</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Mouse</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Printer</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Power</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Monitor</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Cables</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Software patches/hotfixes/updates</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Documentation</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>3.4 Install and configure hardware drivers and devices.</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Imaging devices:</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Barcode scanner</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Document scanner</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Card/badge scanner</td>
<td>5</td>
<td>198-213</td>
</tr>
</tbody>
</table>
### Objective Chapter Pages

<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax printer</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Camera</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Signature pads</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Physical interfaces:</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>USB</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>IEEE 1394</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>SCSI</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Serial</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Mobile storage devices:</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Flash drives</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>External hard drives</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>DVDs</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>CDs</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Tapes</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>SD cards</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Mobile devices:</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Tablet PCs</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Smart phones</td>
<td>5</td>
<td>198-213</td>
</tr>
<tr>
<td>Portable media players</td>
<td>5</td>
<td>198-213</td>
</tr>
</tbody>
</table>

3.5 Compare and contrast basic client networks and tools.

- DHCP vs. static IP                            | 5       | 172-192     |
- Adhoc vs. infrastructure                      | 5       | 172-192     |
- Command line prompts                          | 5       | 172-192     |
  - ping                                        | 5       | 172-192     |
  - ipconfig                                    | 5       | 172-192     |
  - tracert                                     | 5       | 172-192     |

3.6 Setup basic network devices and apply basic configuration settings.

- Wireless access point                         | 5       | 172-192     |
- Security settings                             | 5       | 172-192     |
<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ SSID</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Guest network</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Access point placement</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Router</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ DHCP</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Port forwarding</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Internet modem</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>3.7 Given a scenario, troubleshoot and solve common network problems.</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Cabling</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Power</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ IP settings</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ ISP</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Interference</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>■ Signal issues</td>
<td>5</td>
<td>172-192</td>
</tr>
<tr>
<td>3.8 Explain the features of different backup configurations and the</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>associated maintenance practices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Daily</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ Differential</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ Incremental</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ Archive flags</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>3.9 Classify different server types, environments, features, and</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>limitations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Database server</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ Application server</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ Interfaces</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ Physical connections</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ Server load and utilization</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ Application services</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ OS and application interoperability</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>■ Storage space limitations based on application usage and electronic</td>
<td>5</td>
<td>192-197</td>
</tr>
<tr>
<td>record storage</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 3.10 Compare and contrast EHR/EMR technologies and how each is implemented.

- ASP/Cloud vs. client-server (locally-hosted)  
- Browser vs. installed application vs. terminal/remote access  
- Hardware requirements  

<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.10</td>
<td>5</td>
<td>192-197</td>
</tr>
</tbody>
</table>

### 4.0 Medical Business Operations

#### 4.1 Identify commonly used medical terms and devices.

- Interfaces:
  - HL7
  - e-prescribing
  - CCD
  - CCR
  - ICD10
  - CPT
  - SNOMED
  - NDCID
  - PACS
  - E/M codes
- Devices:
  - Portable x-ray machine
  - MRI
  - Vitals cuff
  - EKG
  - EEG
  - Ultrasound
  - PET
  - CT
  - Vascular/Nuclear Stress Test
  - Glucose monitor
  - Clinical software and modules:
    - Patient tracking

<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>6</td>
<td>227-264</td>
</tr>
<tr>
<td>Objective</td>
<td>Chapter</td>
<td>Pages</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>Scheduling</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>Order entry</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>Practice management</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>Billing/coding</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>Tracking/auditing</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>Basic clinical terms:</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Imaging</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>PCP</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Stat</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Acuity</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Code blue/rapid response</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Trauma levels</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Controlled substance (levels)</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>EHR/EMR</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Common medical departments:</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Inpatient:</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>OBGYN</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>ONC</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>PEDS</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>FBC/L&amp;D/Stork/NICU</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>ICU/CCU</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>TCU/PCU</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>MED/SURG</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Behavior Health</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>PACU</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>OR/UR</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>ER</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>Outpatient</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>OBGYN</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>ONC</td>
<td>6</td>
<td>227-244</td>
</tr>
<tr>
<td>PEDS</td>
<td>6</td>
<td>227-244</td>
</tr>
</tbody>
</table>
Objective Chapter Pages

- Plastic Surgery 6 227-244
- ENT 6 227-244
- Respiratory 6 227-244
- Physical therapy 6 227-244
- Cardiovascular 6 227-244
- Occupational therapy 6 227-244
- Ambulatory/Day surgery 6 227-244
- Radiology 6 227-244
- Laboratory 6 227-244
- Ophthalmology 6 227-244
- Dermatology 6 227-244
- Nuclear 6 227-244

4.2 Explain aspects of a typical clinical environment.

- Basic workflow: 6 227-244
  - Registration 6 227-244
  - Consultation 6 227-244
  - Examination 6 227-244
  - Clinical processes: 6 227-244
    - Computerized physician order entry 6 227-244
    - Transcription 6 227-244
    - Dictation 6 227-244
    - Referrals/consults 6 227-244
    - Digital signatures 6 227-244

4.3 Identify and label different components of medical interfaces.

- HL7: 6 259-264
  - Standard contents 6 259-264
  - Provider types 6 259-264
  - AL1 6 259-264
  - BLG 6 259-264
  - IN1 6 259-264
<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ MSH</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ OBR</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ PID</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ SCH</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ e-prescribing:</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Medication reconciliation</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Bedside medication verification</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Allergy interactions</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Formulary checking</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Billing:</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ EMR/EHR outbound communication</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Types of codes</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Clearinghouse</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>4.4 Determine common interface problems and escalate when necessary.</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ HL7:</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Threads/nodes deactivated</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Improperly formatted patient demographics</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Communication link (fax, network, internet)</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ e-prescribing:</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Improperly formatted patient demographics</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Improperly formatted script</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Deactivated medication</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Controlled substance</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Communication link (fax, network, internet)</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Medical devices:</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Power</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Network</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ I/O</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>■ Configuration settings</td>
<td>6</td>
<td>259-264</td>
</tr>
</tbody>
</table>
**Objective Chapter Pages**

<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing:</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>Improperly formatted patient demographics</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>Improperly formatted superbill</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>Communication link (fax, network, internet)</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>I/O</td>
<td>6</td>
<td>259-264</td>
</tr>
<tr>
<td>Software configuration settings</td>
<td>6</td>
<td>259-264</td>
</tr>
</tbody>
</table>

4.5 Explain the basics of document imaging.

| File types:                                    | 6       | 245-259     |
| TIFF                                          | 6       | 245-259     |
| PDF                                           | 6       | 245-259     |
| JPG                                           | 6       | 245-259     |
| GIF                                           | 6       | 245-259     |
| Characteristics:                              | 6       | 245-259     |
| Quality                                       | 6       | 245-259     |
| Size                                          | 6       | 245-259     |
| Resolution                                    | 6       | 245-259     |
| Compression                                   | 6       | 245-259     |
| Scanning and indexing:                        | 6       | 245-259     |
| Metadata                                      | 6       | 245-259     |
| Storage and retrieval                         | 6       | 245-259     |
| OCR and structured data                       | 6       | 245-259     |

4.6 Given a scenario, determine common clinical software problems.

| Locate the affected modules or fields          | 6       | 245-259     |
| Determine file/data types                      | 6       | 245-259     |
| Escalation procedures to proper support tier   | 6       | 245-259     |
| Vendor or local application support            | 6       | 245-259     |

4.7 Describe change control best practices and its system-wide effects.

<p>| Procedural systematic customization            | 6       | 245-259     |
| Governance board                               | 6       | 245-259     |
| System patching/updates                        | 6       | 245-259     |</p>
<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Appropriate scheduling</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>■ Change control environments:</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>■ Development</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>■ QA/Test</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>■ User test</td>
<td>6</td>
<td>245-259</td>
</tr>
<tr>
<td>■ Production/live</td>
<td>6</td>
<td>245-259</td>
</tr>
</tbody>
</table>

**5.0 Security**

5.1 Explain physical security controls.

■ Locations for:                                                          | 7       | 285-294 |
| ■ Servers                                                                 | 7       | 285-294 |
| ■ Network hardware                                                        | 7       | 285-294 |
| ■ Printers                                                                 | 7       | 285-294 |
| ■ Scanners                                                                | 7       | 285-294 |
| ■ Copiers                                                                 | 7       | 285-294 |
| ■ Access:                                                                 | 7       | 285-294 |
| ■ Servers                                                                 | 7       | 285-294 |
| ■ Office                                                                  | 7       | 285-294 |
| ■ Data closet                                                             | 7       | 285-294 |
| ■ IDF/MDF                                                                  | 7       | 285-294 |
| ■ Backups                                                                  | 7       | 285-294 |
| ■ Keyfobs                                                                 | 7       | 285-294 |
| ■ Badges                                                                  | 7       | 285-294 |
| ■ Biometrics                                                               | 7       | 285-294 |
| ■ Environmental                                                           | 7       | 285-294 |
| ■ HVAC                                                                    | 7       | 285-294 |
| ■ Security lighting                                                       | 7       | 285-294 |
| ■ Surveillance                                                            | 7       | 285-294 |
| ■ Fire suppression                                                        | 7       | 285-294 |
| ■ Personnel                                                               | 7       | 285-294 |
| ■ Generator                                                               | 7       | 285-294 |
5.2 Summarize the different encryption types and when each is used.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types:</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>SSL</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>DES</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>AES</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>3DES</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>PGP</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Communication:</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Email</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Chat</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Smart phone</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Collaboration sites</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>FTP sites</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Phone</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>VoIP</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Fax</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Storage:</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Flash drives</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>PCs</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Laptops</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>SD cards</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>External drives</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Servers</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>Objective</td>
<td>Chapter</td>
<td>Pages</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>■ NAS</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>■ SANS</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>■ Dissemination of PHI</td>
<td>7</td>
<td>296-301</td>
</tr>
<tr>
<td>5.3 Apply best practices when creating and communicating passwords.</td>
<td>7</td>
<td>294-295</td>
</tr>
<tr>
<td>■ Communication of passwords</td>
<td>7</td>
<td>294-295</td>
</tr>
<tr>
<td>■ Storage of passwords</td>
<td>7</td>
<td>294-295</td>
</tr>
<tr>
<td>■ Password strength (complexity/length)</td>
<td>7</td>
<td>294-295</td>
</tr>
<tr>
<td>■ Password reuse</td>
<td>7</td>
<td>294-295</td>
</tr>
<tr>
<td>5.4 Classify permission levels based on roles.</td>
<td>7</td>
<td>283-285</td>
</tr>
<tr>
<td>■ Read</td>
<td>7</td>
<td>283-285</td>
</tr>
<tr>
<td>■ Write</td>
<td>7</td>
<td>283-285</td>
</tr>
<tr>
<td>■ Modify</td>
<td>7</td>
<td>283-285</td>
</tr>
<tr>
<td>■ Full access</td>
<td>7</td>
<td>283-285</td>
</tr>
<tr>
<td>5.5 Identify different remote access methods and security controls.</td>
<td>7</td>
<td>303-306</td>
</tr>
<tr>
<td>■ RDC</td>
<td>7</td>
<td>303-306</td>
</tr>
<tr>
<td>■ VPN</td>
<td>7</td>
<td>303-306</td>
</tr>
<tr>
<td>■ Remote control applications</td>
<td>7</td>
<td>303-306</td>
</tr>
<tr>
<td>■ Terminal emulation</td>
<td>7</td>
<td>303-306</td>
</tr>
<tr>
<td>■ L2TP</td>
<td>7</td>
<td>303-306</td>
</tr>
<tr>
<td>■ SSH</td>
<td>7</td>
<td>303-306</td>
</tr>
<tr>
<td>■ HTTPS</td>
<td>7</td>
<td>303-306</td>
</tr>
<tr>
<td>■ SFTP</td>
<td>7</td>
<td>303-306</td>
</tr>
<tr>
<td>5.6 Recognize wireless security protocols and best practices.</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>■ WEP</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>■ WPA</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>■ WPA2</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>■ AES</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>■ RADIUS</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>■ SSID naming</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>■ MAC filtering</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>Objective</td>
<td>Chapter</td>
<td>Pages</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Site surveys</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>Access point placement</td>
<td>7</td>
<td>302-303</td>
</tr>
<tr>
<td>5.7 Implement best practices in secure disposal of electronic or physical PHI.</td>
<td>7</td>
<td>307-308</td>
</tr>
<tr>
<td>Secure shredding</td>
<td>7</td>
<td>307-308</td>
</tr>
<tr>
<td>Degaussing</td>
<td>7</td>
<td>307-308</td>
</tr>
<tr>
<td>Sanitizing</td>
<td>7</td>
<td>307-308</td>
</tr>
<tr>
<td>5.8 Implement backup procedures based on disaster recovery policies.</td>
<td>7</td>
<td>306-307</td>
</tr>
<tr>
<td>Deployment, configuration and testing of backups</td>
<td>7</td>
<td>306-307</td>
</tr>
<tr>
<td>Backup storage:</td>
<td>7</td>
<td>306-307</td>
</tr>
<tr>
<td>Offsite</td>
<td>7</td>
<td>306-307</td>
</tr>
<tr>
<td>Courier</td>
<td>7</td>
<td>306-307</td>
</tr>
<tr>
<td>Onsite</td>
<td>7</td>
<td>306-307</td>
</tr>
<tr>
<td>Methods of secure transfer</td>
<td>7</td>
<td>306-307</td>
</tr>
<tr>
<td>Backup inventory</td>
<td>7</td>
<td>306-307</td>
</tr>
<tr>
<td>5.9 Identify common security risks and their prevention methods.</td>
<td>7</td>
<td>281-283</td>
</tr>
<tr>
<td>Social engineering—User training</td>
<td>7</td>
<td>281-283</td>
</tr>
<tr>
<td>Phishing—User training</td>
<td>7</td>
<td>281-283</td>
</tr>
<tr>
<td>Spamming—Filters</td>
<td>7</td>
<td>281-283</td>
</tr>
<tr>
<td>Malware—Access control</td>
<td>7</td>
<td>281-283</td>
</tr>
<tr>
<td>Spyware—Anti-spyware</td>
<td>7</td>
<td>281-283</td>
</tr>
</tbody>
</table>
Introduction

Welcome to the *CompTIA Healthcare IT Technician HIT-001 Cert Guide*. The CompTIA Healthcare IT Technician certification was created due to a growing need for it in the healthcare IT field. The CompTIA Healthcare IT Technician certification is designed to be a vendor-neutral exam that measures your knowledge of industry-standard technologies and methodologies. It serves as a gateway to transition from IT into healthcare IT. This book was developed to be a resource while studying for the exam and also to be a reference while working on the job.

The Healthcare IT Technician exam objectives were designed with the suggestion that the test taker would already have the CompTIA A+ certification. Although having the CompTIA A+ certification before attempting the CompTIA Healthcare IT Technician exam can greatly benefit you, the book does review and explain the CompTIA A+ objectives as needed to pass the exam.

While writing this book, the author imagined how to share what she knows with a new employee at the healthcare company where she used to work. Most new employees have a strong IT background but don’t actually have much experience on the medical side of healthcare IT. This book completes a picture from IT to healthcare IT.

Good luck as you explore the new world of healthcare IT and prepare to take the CompTIA Healthcare IT Technician exam. As you read this book you can learn how to combine two worlds into a familiar environment, armed with knowledge and skills to pass the exam.

Goals and Methods

The number one goal of this book is to help you pass the 2011 version of the CompTIA Healthcare IT Technician certification exam (number HIT-001).

The CompTIA Healthcare IT Technician certification exam involves familiarity with healthcare and the information systems used in the healthcare environment. To aid you in mastering and understanding the Healthcare IT Technician certification objectives, this book uses the following methods:

- **Opening topics list:** This defines the topics covered in the chapter; it also lists the corresponding CompTIA Healthcare IT Technician objective numbers.
- **Topical coverage**: The heart of the chapter that explains each objective from a practical perspective relative to the exam and potential future jobs. This includes in-depth descriptions, tables, and figures geared to build your knowledge so that you can pass the exam. The chapters are broken down by objective domains.

- **Exam Tips**: The Exam Tips indicate important subjects, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter.

- **Notes**: The Notes offer bits of information that help you to understand a topic covered or direct you to where you can find more information on a topic.

- **Key Terms**: Key Terms are definitions of important vocabulary you need to know to pass the exam and succeed in healthcare IT. Key terms are interspersed throughout the chapter and listed without definitions at the end of each chapter.

- **HIT in the Real World**: Each chapter has a story that provides a real-world experience. These stories demonstrate at least one topic covered in the chapter and how it is important to learn the objectives for success in healthcare IT.

- **Chapter Summary**: At the end of each chapter, you can find a summary of the key topics covered in the chapter.

- **Acronym Drill**: In healthcare IT there are so many acronyms it is easy to get confused by them. The acronym drill reinforces learning the acronyms so that they become second nature.

- **Review Questions**: At the end of each chapter is a quiz. The quizzes, and answers with explanations, are meant to gauge your knowledge of the subjects. If an answer to a question doesn't come readily to you, be sure to review that portion of the chapter.

- **Practical Application**: There are critical thinking questions at the end of each chapter. These questions or challenges are intended to put to use what you have learned in the chapter to reinforce your learning the content of the chapter.

---

**Who Should Read This Book?**

This book is for anyone who wants to start or advance a career in healthcare IT. Readers of this book can range from persons taking a healthcare IT course to individuals already in the field who want to keep their skills sharp. Many readers will be individuals who have earned the CompTIA A+ certification and want to broaden
into healthcare for more job opportunities. This book is designed to offer an easy transition from IT to healthcare IT.

This book also offers opportunity for individuals in healthcare to transition into healthcare IT. This book offers an IT background of all objectives. Whether your background is in healthcare or IT, this book prepares you for the CompTIA Healthcare IT Technician exam.

Although not a prerequisite, CompTIA Healthcare IT Technician candidates should have at least one year of technical experience. The CompTIA A+ certification is also recommended as a prerequisite. It is expected that you understand basic computer topics such as how to install operating systems and applications and so on. The focus of this book is on the technologies used in the healthcare environment and the rules and regulations about how to use these technologies.

Important! If you do not feel that you have the required experience or are new to the IT field, consider an IT course that covers the CompTIA Healthcare IT Technician objectives. You can choose from plenty of technical training schools, community colleges, and online courses. Use this book with the course and any other course materials you obtain.

**CompTIA Healthcare IT Technician Exam Topics**

Table I-1 lists the exam topics for the CompTIA Healthcare IT Technician exam. This table lists the chapter in which each exam topic is covered. Chapters 1 and 2 are introductory chapters and as such do not map to any specific exam objectives.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Exam Topic</th>
<th>CompTIA Healthcare IT Technician Exam Objectives Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview of the HITECH Act, healthcare, and healthcare IT.</td>
<td>Applies to the entire exam.</td>
</tr>
<tr>
<td>2</td>
<td>Overview of data flow used in healthcare information systems.</td>
<td>Applies to the entire exam.</td>
</tr>
<tr>
<td>Chapter</td>
<td>Exam Topic</td>
<td>CompTIA Healthcare IT Technician Exam Objectives Covered</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>Identify standard agencies, laws, and regulations.</td>
<td>Objectives 1.1, 1.2, 1.3, 1.4</td>
</tr>
<tr>
<td></td>
<td>Explain and classify HIPAA controls and compliance issues.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Summarize regulatory rules of record retention, disposal, and archiving.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain and interpret legal best practices, requirements, and documentation.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Use best practices for handling PHI in the workplace.</td>
<td>Objective 2.1, 2.2, 2.3, 2.4, 2.5</td>
</tr>
<tr>
<td></td>
<td>Identify EHR/EMR access roles and responsibilities.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apply proper communication methods in the workplace.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify organizational structures and different methods of operation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Given a scenario, execute daily activities while following a code of conduct.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Identify commonly used IT terms and technologies.</td>
<td>Objectives 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10</td>
</tr>
<tr>
<td></td>
<td>Demonstrate the ability to set up a basic PC workstation within an EHR/EMR environment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Given a scenario, troubleshoot and solve common PC problems.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Install and configure hardware drivers and devices.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compare and contrast basic client networks and tools.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set up basic network devices and apply basic configuration settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Given a scenario, troubleshoot and solve common network problems.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the features of different backup configurations and the associated maintenance practices.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Classify different server types, environments, features, and limitations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compare and contrast EHR/EMR technologies and how each is implemented.</td>
<td></td>
</tr>
<tr>
<td>Chapter</td>
<td>Exam Topic</td>
<td>CompTIA Health-care IT Technician Exam Objectives Covered</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>Identify commonly used medical terms and devices.</td>
<td>Objectives 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7</td>
</tr>
<tr>
<td></td>
<td>Explain aspects of a typical clinical environment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify and label different components of medical interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determine common interface problems and escalate when necessary.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Explain the basics of document imaging.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Given a scenario, determine common clinical software problems.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Describe change control best practices and its system-wide effects.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Explain physical security controls.</td>
<td>Objectives 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9</td>
</tr>
<tr>
<td></td>
<td>Summarize the different encryption types and when each is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apply best practices when creating and communicating passwords.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Classify permission levels based on roles.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify different remote access methods and security controls.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recognize wireless security protocols and best practices.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implement best practices in secure disposal of electronic or physical PHI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implement back-up procedures based on disaster recovery policies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify common security risks and their prevention methods.</td>
<td></td>
</tr>
</tbody>
</table>

**Pearson IT Certification Practice Test Engine and Questions on the CD**

The CD in the back of the book includes the Pearson IT Certification Practice Test engine software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode or taking a simulated exam that mimics real exam conditions.
The installation process requires two major steps: installing the software and then activating the exam. The CD in the back of this book has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam—the database of exam questions—is not on the CD.

NOTE The cardboard CD case in the back of this book includes the CD and a piece of paper. The paper lists the activation code for the practice exam associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Install the Software from the CD
The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows Virtual Machine, but it was built specifically for the PC platform. The minimum system requirements follow:

- Windows XP (SP3), Windows Vista (SP2), or Windows 7
- Microsoft .NET Framework 4.0 Client
- Microsoft SQL Server Compact 4.0
- Pentium class 1GHz processor (or equivalent)
- 512 MB RAM
- 650 MB disc space plus 50 MB for each downloaded similar to other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, you do not need to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the CD sleeve.

The following steps outline the installation process:

Step 1: Insert the CD into your PC.

Step 2: The software that automatically runs is the Pearson software to access and use all CD-based features, including the exam engine and the appendix. From the main menu, click the Install the Exam Engine option.

Step 3: Respond to windows prompts as with any typical software installation process.
The installation process gives you the option to activate your exam with the activation code supplied on the paper in the CD sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so register when prompted. If you already have a Pearson website login, you do not need to register again; just use your existing login.

**Activate and Download the Practice Exam**

After the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

- **Step 1:** Start the Pearson IT Certification Practice Test software from the Windows **Start** menu or from your desktop shortcut icon.
- **Step 2:** To activate and download the exam associated with this book, from the My Products or Tools tab, select the **Activate** button.
- **Step 3:** At the next screen, enter the Activation Key from the paper inside the CD sleeve in the back of the book. When it’s entered, click the **Activate** button.
- **Step 4:** The activation process downloads the practice exam. Click **Next**, and then click **Finish**.

After the activation process completes, the My Products tab should list your new exam. If you do not see the exam, make sure you have selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab, and select the **Update Products** button. Updating your exams ensures you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, simply select the **Tools** tab, and select the **Update Application** button. This ensures you are running the latest version of the software engine.

**Activating Other Exams**

The exam software installation process, and the registration process, must happen only once. Then, for each new exam, only a few steps are required. For instance, if you buy another new Pearson IT Certification Cert Guide or Cisco Press Official Cert Guide, extract the activation code from the CD sleeve in the back of that book—you don’t need the CD at this point. From there, all you need to do is start the exam engine (if it’s not still up and running), and perform steps 2 through 4 from the previous list.
**Premium Edition**

In addition to the two free practice exams provided on the CD, you can purchase one additional exam with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional full practice exam as well as an eBook (in both PDF and ePub format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

If you purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the CD sleeve that contains a one-time-use code as well as instructions for where you can purchase the Premium Edition.

This page intentionally left blank
CHAPTER 3

Regulatory Requirements

In this chapter you learn about:

- Agencies, laws, and regulations
- HIPAA controls and compliance issues
- Types of health records and rules of record retention and disposal
- Legal best practices, requirements, and documentation

Regulatory requirements don’t sound like fun to read about. No matter how boring this topic is, it is relevant to HIT. The requirements keep you and others out of trouble. The agencies and laws are in place to protect patients’ rights and privacy and help you find resources.

Laws and regulations change and can be updated, so the most important point of this chapter is to know where to go to find current information. Also agencies, laws, and regulations vary from state to state, so you need to be aware of local policies in your state.

Use government websites and Internet search engines to find information. The government or .gov sites are the authoritative sources. Other websites might offer insight about where to look for answers or how other facilities handle issues. If you cannot find what you need, look within your facility. Often all it takes to find information about a policy is to visit the department in your hospital that handles matters of policy on a daily basis.

This chapter begins by identifying and explaining the roles of some important agencies and laws.
Identifying Standard Agencies, Laws, and Regulations

HI001 Objectives:

1.1 Identify standard agencies, laws, and regulations.

HHS, ONC, CMS, HIPAA, Medicare, Medicaid, ARRA, HITECH, Meaningful use, Eligible provider, NIST

EXAM TIP Notice all the acronyms as you read this book. Pay attention to them because you absolutely will see them again on the exam and on the job.

Each of the agencies, laws, and regulations described in the following sections play a role in healthcare. The agencies of the U.S. government are responsible for implementing the laws and regulations created by Congress and enacted by the President. The common goal of the agencies, laws, and regulations is to improve the healthcare available to citizens. First, learn about the agencies.

Agencies Governing Healthcare

With changes in the government over the last few years, generous resources have been provided for the development and implementation of HIT. The government has focused funding toward advancing healthcare technology in the United States. The government created agencies to filter the monies to covered entities. Covered agencies work toward this same goal to advance healthcare technology. The government and covered agencies are tasked with ensuring the laws and regulations have compliance by healthcare providers and facilities.

covered entity—Health Insurance Portability and Accountability Act (HIPAA) is designed to protect health information used by health insurance plan providers, healthcare clearinghouses, and healthcare providers. These three entities are classified as covered entities. Basically, a covered entity is anyone or any organization required to submit to HIPAA rules.

Health Insurance Portability and Accountability Act (HIPAA)—A law created in 1996 to provide a standard set of rules that all covered entities must follow to protect patient health information and to help healthcare providers transition from paper to electronic health records.
Following is a list of agencies that govern healthcare in the United States:

- Department of Health and Human Services (HHS)
- National Institute of Standards and Technology (NIST)

**Department of Health and Human Services**

The Department of Health and Human Services (HHS)—http://www.hhs.gov—is an agency of the U.S. government tasked with the following responsibilities:

- Protect the health of Americans.
- Provide a means for Americans who are least able to help themselves to access healthcare.
- Contain and treat any national health emergencies.
- Test and regulate food and drug supplies.

Figure 3-1 shows the HHS website.
Chapter 3: Regulatory Requirements

The HHS website is current and informative with the need-to-know facts and how to access resources the HHS provides.

Photo credit: http://www.hhs.gov

The HHS contains several operating divisions, as shown in Table 3-1.

### Table 3-1 Operating Divisions of the HHS

<table>
<thead>
<tr>
<th>Division</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration for Children and Families</td>
<td>ACF</td>
</tr>
<tr>
<td>Administration on Children, Youth, and Families</td>
<td>ACYF</td>
</tr>
<tr>
<td>Administration on Aging</td>
<td>AoA</td>
</tr>
<tr>
<td>Agency for Healthcare Research and Quality</td>
<td>AHRQ</td>
</tr>
</tbody>
</table>
The more notable divisions of the HHS include the Food and Drug Administration (FDA), Centers for Disease Control and Prevention (CDC), and the National Institutes of Health (NIH). Now take a closer look at the divisions of the HHS involved in healthcare:

- Centers for Medicare & Medicaid Services (CMS)
- Office of the National Coordinator for HIT (ONC)
- Office for Civil Rights (OCR)

### Centers for Medicare & Medicaid Services (CMS)

The Centers for Medicare & Medicaid Services (CMS) branch—http://www.cms.gov—of the HHS is responsible for administrating Medicare and Medicaid. CMS also regulates the transaction standards of billing codes used to price healthcare expenses, such as electronic claims, remittance, eligibility, and claims status requests/responses. The current version of HIPAA transaction standards is **Version 5010**. All HIPAA-compliant facilities adopted this version January 1, 2012. CMS regulates medical diagnosis and inpatient procedure coding in healthcare. The current version is **ICD-9**. The new version, **ICD-10**, is required to be adopted by HIPAA-compliant facilities by October 1, 2013. Figure 3-2 shows the CMS website homepage.

---

**Table 3-1** Continued

<table>
<thead>
<tr>
<th>Division</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centers for Disease Control and Prevention</td>
<td>CDC</td>
</tr>
<tr>
<td>Centers for Medicare &amp; Medicaid Services</td>
<td>CMS</td>
</tr>
<tr>
<td>Food and Drug Administration</td>
<td>FDA</td>
</tr>
<tr>
<td>Health Resources and Services Administration</td>
<td>HRSA</td>
</tr>
<tr>
<td>Indian Health Service</td>
<td>IHS</td>
</tr>
<tr>
<td>National Institutes of Health</td>
<td>NIH</td>
</tr>
<tr>
<td>National Cancer Institute</td>
<td>NCI</td>
</tr>
<tr>
<td>Office of the Inspector General</td>
<td>OIG</td>
</tr>
<tr>
<td>Substance Abuse and Mental Health Services Administration</td>
<td>SAMHSA</td>
</tr>
</tbody>
</table>
Version 5010—HIPAA mandated a standard format for electronic claims transactions. This standard was updated to grow with the functional needs of the healthcare industry. The http://www.cms.gov website offers more details about Version 5010.

ICD-9—HIPAA mandated a standard format for electronic provider and diagnostic codes. The current standard has limitations that restrict the full use of EMR/EHR software.

ICD-10—HIPAA mandated a standard electronic format for provider and diagnostic codes. The new standard is intended to grow with the functional needs of the healthcare industry. The http://www.cms.gov website offers more details about ICD-10.

Figure 3-2  The CMS website is current and informative with the need-to-know facts and how to access resources the CMS provides.

Photo credit: http://www.cms.gov
The purpose of coding is to equate expenses in a hospital into numbers. For example, whenever a doctor examines a patient, a nurse uses a syringe to administer a drug, or a patient receives a diagnosis, a code must be generated to represent the expense associated with providing this patient care. When healthcare providers enter information into a patient’s chart, that information eventually is sent to a medical coding specialist. This person is responsible for translating charted documentation about a patient’s stay in a hospital into codes so that insurance companies can be properly billed for the hospital’s expenses.

Covered entities must upgrade to Version 5010 billing codes to be prepared for the ICD-10 diagnostic and procedure codes. ICD-10 codes accommodate Version 5010. The reason for the transition to Version 5010 over a year and a half before the transition to ICD-10 is to make sure any kinks in the transition to Version 5010 have been addressed to reduce the possibilities of problems in the transition to ICD-10.

The need for the transition from ICD-9 to ICD-10 is because ICD-9 is too restrictive in the amount of information the code can communicate. With ICD-10, a code can report more specifically what was wrong with a patient and how the patient was treated. ICD-10 uses more character fields in the code and approximately 55,000 more available codes. For example, if a physician charts “initial encounter for a stress fracture of the right tibia,” in ICD-9, a coder could use only the code 733.9 to mean the limited information “stress fracture of the tibia.” This ignores a lot of specific information about this patient’s condition. Because this was the first encounter and of the right tibia would be coded using separate codes. With ICD-10, the coder can report more details in a single code using a longer code with more options to choose from. To report “initial encounter for a stress fracture of the right tibia” in ICD-10, a coder would report M84.361A as the code.

Office of the National Coordinator for Health Information Technology (ONC)
Office of the National Coordinator for Health Information Technology (ONC)—http://www.healthit.hhs.gov: This office of the HHS was created to promote national HIT infrastructure and oversee its development. The ONC was created by executive order in 2004 and written into legislation by the HITECH Act in 2009, which requires healthcare providers to move toward using electronic solutions to store and process patient data. The ONC tests and certifies all EMR/EHR solutions to be HIPAA-compliant. Healthcare providers and hospitals may use only the certified EMR/EHR solutions if they want to qualify for monetary incentives. Figure 3-3 shows the ONC website.
The U.S. government provides funding through various venues to encourage covered entities to transition to advanced healthcare technology. Covered entities are encouraged to meet deadlines for stages in the transition, for example, to EMR/EHR information systems. If they meet these goals, they are given money. The deadlines for the incentives are set before the deadlines of when covered entities are required to transition to advanced healthcare technology. If a covered entity misses the latter required deadline, the U.S. government starts applying penalties for not complying with the required deadline. It serves the covered entities well to be ahead of the game by transitioning to advanced healthcare technologies sooner rather than later.
Office of Civil Rights (OCR)

Office of Civil Rights (OCR)—http://www.hhs.gov/ocr: This office of the HHS is responsible to protect Americans against discrimination and enforce the Privacy and Security Rules of HIPAA. The OCR fulfills this responsibility through education to prevent violations and through investigation of complaints about violations of these rules. The OCR usually enables a covered entity to enforce rules and reprimand violations without intervening. Complaints about violations are filed through the OCR. See Figure 3-4 to see the OCR website.

Figure 3-4  The OCR website is current, informative, and offers instructions on how to file a complaint about a privacy violation.

Photo credit: http://www.hhs.gov/ocr

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST)—http://www.nist.gov—This agency is part of the U.S. Department of Commerce. The goal of the NIST is to promote
U.S. innovation and industrial competition. The NIST aims to advance standards and technology to improve American economic security and quality of life. In healthcare, the NIST aims to do the following:

- Create opportunities for accelerated research and development of HIT.
- Improve the usefulness of HIT and remote healthcare.
- Develop the security of HIT.

Figure 3-5 shows the NIST website.

Figure 3-5  The NIST website is current and informative of its activities.

Photo credit: http://www.nist.gov

EXAM TIP  Expect to see the NIST on the Healthcare IT exam in the context of how it aims to improve healthcare IT.
Now that you have learned about the agencies for healthcare, turn your attention to the programs and laws that these agencies offer and enforce.

**Healthcare Programs**

Government agencies use social programs to fulfill responsibilities tasked to the agency. Programs ensure accessibility of benefits to those who qualify. The two most significant healthcare programs are Medicare and Medicaid. Medicare and Medicaid are impressive by the numbers of beneficiaries and expense.

The Medicare—http://www.medicare.gov—social insurance program is for hospital and medical care for elderly and certain disabled citizens. Medicare is provided by the U.S. government. Medicare was created as an amendment to the Social Security Act in 1965. Medicare is regulated and administered at the federal level. Figure 3-6 shows the Medicare website homepage.

![Figure 3-6](http://www.medicare.gov)

The Medicare website is current and informative with the need-to-know facts and how to access resources Medicare provides.

Photo credit: http://www.medicare.gov
The Medicaid—http://www.medicaid.gov—social welfare program is for health and medical services for certain citizens and families with low incomes and few resources. Medicaid is provided by the U.S. government. Medicaid was created as an amendment to the Social Security Act in 1965. Primary oversight of Medicaid is regulated at the federal level. All states participate in Medicaid; however, state participation to use Medicaid funding is voluntary. Each state administers this program using Medicaid funding. States also have control over eligibility standards, scope of services, and rate of payment for services. Figure 3-7 shows the Medicaid website.

**Figure 3-7** The Medicaid website is current and informative with the need-to-know facts and how to access resources Medicaid provides.

Photo credit: http://www.medicaid.gov
Healthcare Laws

Government agencies use laws to define the scope of responsibilities tasked to the agency. Laws clarify the manner and intent of the government. HIPAA, ARRA, and HITECH are all acts of Congress meant to improve healthcare in the United States.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA)—http://www.hhs.gov/ocr/privacy—was created in 1996 to provide a standard set of rules for all covered entities to follow to protect patient health information and to help healthcare providers transition from paper to electronic health records. The Office of Civil Rights (OCR) enforces the following HIPAA rules:

- **Privacy Rule**: Establishes national standards to protect individuals’ health information whenever a covered entity accesses this information. This rule establishes safeguards to regulate who can access **e-PHI (electronic protected health information)** and the reasons why someone needs to access e-PHI.

- **Security Rule**: Establishes national standards to protect the e-PHI of an individual. This rule establishes safeguards for how e-PHI is accessed.

- **Breach Notification Rule**: Requires covered entities to notify affected individuals, the HHS secretary, and possibly the media when protected health information (PHI) has been breached.

- **Enforcement Rule**: Establishes penalties for violations to HIPAA rules and procedures following a violation, such as investigations and hearings.

Figure 3-8 shows the enforcement activities and results on the HIPAA website.
Figure 3-8 The HIPAA website is current and informative of the need-to-know facts.

Photo credit: http://www.hhs.gov/ocr/privacy/hipaa/enforcement

American Recovery and Reinvestment Act (ARRA)

The American Recovery and Reinvestment Act (ARRA)—http://www.recovery.gov—was created in 2009 at the urging of President Obama to help citizens through the economic recession. This act is called the Recovery Act. The Recovery Act provided hundreds of billions of dollars for tax cuts, funding for entitlement programs, and federal contracts, grants, and loans. Specific to healthcare, the Recovery Act provides funding to HHS branches, such as the CMS and ONC. The Recovery Act is intended to help preserve and improve affordable healthcare in the United States. The Recovery Act also creates plans and incentives to assist Americans through challenges faced as a nation. Figure 3-9 shows the Recovery Act website.
Figure 3-9  The Recovery Act website is current and informative with the need-to-know facts and how to access resources the Recovery Act provides.

Photo credit: http://www.recovery.org

EXAM TIP  For the Healthcare IT exam, you need to know how the ARRA has affected healthcare and healthcare IT.

Health Information Technology for Economic and Clinical Health (HITECH) Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act—http://www.healthit.hhs.gov—focuses on creating incentive and opportunity for the advancement of HIT through the ONC. The programs funded in the HITECH Act collectively aim to make EMRs/EHRs relevant and beneficial resources to all Americans. The HITECH Act provides grants for education
programs and monetary incentives. The HITECH Act also encourages communication within the healthcare community, within a state, and between states as HIT is advanced and implemented.

**EXAM TIP** For the Healthcare IT exam, you need to know about the HITECH Act and how its funding and regulations affect healthcare and healthcare IT.

Now that you are familiar with programs and laws about healthcare, the following sections explain how these programs and laws are regulated.

**Regulations of Healthcare Laws**

Government agencies use regulations to ensure the intent of the government is carried out. It is in these regulations that healthcare providers and hospitals begin to understand the means and extent of the laws’ intent.

Two new buzzwords in HIT are **meaningful use** and **eligible provider**. The Recovery Act requires covered entities to use HIT in a meaningful way, which is where the term “meaningful use” came from. The meaningful use of HIT justifies the push to advance in technology and offer incentives to accomplish this goal. Starting in 2011, grants from the HITECH Act provide incentives with deadlines for healthcare providers to comply with the regulations identified by meaningful use. By 2015, all healthcare entities must demonstrate meaningful use to avoid financial penalties. Eligible providers are covered entities that want to receive monetary incentives by meeting meaningful use criteria. This qualification makes them eligible to receive incentive money.

**meaningful use**—The goals of meaningful use are to help healthcare providers know more about their patients, make better decisions, and save money by using HIT in a meaningful way.

**eligible provider**—Hospitals or professionals participating in incentive programs must meet meaningful use criteria to be eligible to receive incentive money.

**EXAM TIP** To pass the Healthcare IT exam, you need to understand the terms “meaningful use” and “eligible provider” and use both terms appropriately when discussing how the ARRA has affected healthcare IT.
Now that you know some background on the agencies, laws, and regulations, the following section shifts the focus to how the agencies and acts from the government regulate privacy.

# Learning HIPAA Controls and Compliance Issues

The HHS publishes rules and regulations through HIPAA to provide standards that control and require compliance for the security of e-PHI. HIPAA Privacy and Security Rules provide the regulations that covered entities must follow to protect e-PHI. The HIPAA Enforcement Rule explains the consequences of violating the Privacy and Security Rules. These three rules are not just technical safeguards but also physical and administrative safeguards, including auditing, enforcement, and punishment standards. To fully understand these rules, you must understand the issues concerning these rules and the reasons for creating the rules. The following issues are explained as they relate to HIPAA.

- **Security**: Keeping e-PHI secure is a concern for HIPAA because HIPAA is designed to protect e-PHI. The security measures include all the administrative, physical, and technical safeguards in any IS containing or processing e-PHI. This includes security protocols that HIT technicians must follow, such as administrating security access.

  HIPAA security protects e-PHI created, received, used, or maintained by a covered entity. The OCR is responsible for enforcing HIPAA security. The following portions of HIPAA security ensure the confidentiality, integrity, and availability of e-PHI.

- **Violations**: The breach of a HIPAA rule must be defined for covered entities to know boundaries of what is not acceptable behavior to maintain privacy of patients. A breach can be theft, unauthorized access or disclosure, loss, or improper disposal of e-PHI.

- **Fines**: Normally, the OCR does not intervene when there is a violation to HIPAA rules. Instead, the covered entity that violates the rule issues voluntary compliance and corrective action that reaches a satisfactory resolution with the
OCR. If the violating entity does not handle the offense properly, there are monetary penalties. HIPAA states the fine for each incident should not exceed $100 or $25,000 for identical violations within a calendar year. In 2009, the ARRA increased these amounts into a tiered structure, as outlined in Table 3-2.

Table 3-2 The ARRA Defines These Penalties If a Covered Entity Violates a HIPAA Rule

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA.</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect.</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period.</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected.</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>

- **Requirements**: States have the capability to tighten the rules for security. When you start a new job, especially if you are in a new state, be sure to check with your local state regulations because the state may have different rules than what you knew from your last job. Covered entities must
  - Ensure confidentiality, integrity, and availability of e-PHI they create, receive, maintain, or transmit.
  - Identify risks to e-PHI and implement resolutions to anticipated threats.
  - Ensure compliance by their workforce.

HIPAA enables certain hospital personnel to access patient information to perform job duties. However, if a patient wants his patient information released to a person or organization that is not a covered entity, the covered entity must receive written permission to access and distribute the e-PHI.

This website shows an example of a release form used in New York: [http://www.nycourts.gov/forms/Hipaa_fillable.pdf](http://www.nycourts.gov/forms/Hipaa_fillable.pdf). For example, a patient might need this form to release medical information to an athletic program.
A covered entity might access e-PHI to distribute to the individual or its own personnel for treatment of the patient or to retrieve payment from the patient’s insurance provider without acquiring a release form. Access permission is restricted based on the role of the personnel, called role-based access control. Personnel should have access to e-PHI only as required to fulfill their job descriptions, no more, no less. Ultimately the CFO has the final say in what access to the information systems used in the hospital is granted to hospital personnel. The CFO makes these determinations by approving access to each job role when each IS is initially configured. Therefore, the CFO does not need to be involved with assignments for each employee. When a professional starts a job at a healthcare facility, he is given access to e-PHI as defined by his job. For example, all lab technicians should have access as defined for a lab technician. All nurses should have access as defined for a nurse. A lab technician and a nurse might not have the same access. While performing duties of their job, these personnel do not require signed release forms from patients. The personnel is required to sign an acknowledgment of understanding HIPAA rules. These access policies are controlled by the covered entity and are expected to comply with HIPAA and state regulations.

The HHS offers case studies of HIPAA violations on its website. An example of one case study was a hospital employee who left a voicemail for a patient on the patient’s home answering machine. The message included the medical condition and treatment plan of the patient. However the patient did not live alone and others in the household listened to the message. The patient had specifically asked to be contacted at her work phone number. The hospital employee did not follow confidential communication requirements as set by the hospital. To resolve this violation, the hospital implemented new policies for communication. For example, the policy set rules for the minimum information required to leave in a voicemail so as to not reveal PHI. The hospital also trained employees how to review registration information from patients to verify special instructions from the patient on how to contact them. Finally, the hospital integrated training for these new policies into the annual refresher series for employees.

With the background surrounding agencies, laws, and regulations covered, now turn your focus to a topic a little more practical: the rules of record retention and disposal.
Learning Rules of Record Retention and Disposal

HI001 Objectives:

1.3 Summarize regulatory rules of record retention, disposal, and archiving.

Documentation requirements, Time of storage, Types of records, Public records, Private records, Legal health record, Methods of record disposal

Documentation requirements are defined by HIPAA, but some requirements vary from state to state. The state defines how long records must be kept, called record retention. HIPAA defines how records are disposed of and how they are kept in storage (archived). The three types of records are public, private, and legal. All these follow the same rules for retention and disposal.

Types of Health Records

Health information comes in three different types. A patient’s public health record is used for research and to create reports for public health data. For example, if a state requires a hospital to report how many patients are at risk for getting the flu, the public health records are accessible to calculate this information. Figure 3-10 shows the reporting function of an example EHR IS. Public health records are not intended to connect individuals to their health records.

public health record—Researchers need access to health records to analyze data. For this reason a public health record is made available for the collection of public health data in an anonymous manner.

A private health record is the health record created and maintained by an individual. The benefit of a private health record is the individual is completely aware of all healthcare received and is available to the individual no matter where she may be a patient. A private health record is great for chronically ill patients or for an individual who is a guardian of another individual.
Figure 3-10  The reporting feature of an EHR IS provides a list of patients at risk for the H1N1 virus.

Photo credit: http://www.practicefusion.com

private health record—A health record created and maintained by an individual. Sometimes called a personal health record (PHR).

An individual may keep a private health record in any format she prefers. She may simply place her health records in a file folder on her computer or move it to a jump drive for added security and mobility. She might decide to keep her health records with a web-based service designed for private health records. The benefit of using a web-based service is that many healthcare providers can access and easily format the data from these services for the HIS used at the facility with the permission from the individual.

A legal health record is the health record created by healthcare providers. The regulations for legal health records are set by the state and healthcare organization with a few basic standards set by the federal government. The legal health record can be requested by the patient or legal services. For example, if a patient brings up a lawsuit due to received healthcare, the court might need the legal health record to know what was charted in the patient’s health record.
Record Retention

HIPAA sets a minimum timeframe for record retention of six years and for two years after a patient’s death, and Medicare requires Medicare beneficiaries’ records be retained for five years. HIPAA enables the states to create laws to dictate their own policy for record retention so long as the state law meets minimum HIPAA requirements. If a state requires more time for record retention, covered entities in that state must comply with the state law.

States have the freedom to determine how long documents need to be stored before disposal. States retain records anywhere from 6 to 20 years. Some states choose to vary the length of record retention based on resources, type of patient, events during the course of care, or any other stipulation.

When you start a new job, check with your state’s legislature website or ask someone in the medical records department at your facility. For example, if your new job is to implement a new EMR/EHR IS in a hospital, you would need to know how long to program the EMR/EHR IS to retain the health records.

Record Disposal

HIPAA states that record disposal is the responsibility of covered entities. Physical documentation can be shredded, burned, or pulverized. PHI on electronic media is sometimes disposed of by cleaning, purging, or destroying the device. The covered entity is at fault if any physical or electronic PHI is recovered at any point after the disposal of records.

The basic rule when disposing of an electronic device that contained e-PHI is to make sure the data on the device is unreadable, is indecipherable, and cannot be reconstructed. Following are three ways records on electronic media can be disposed of:

- Cleaning the device is when irrelevant data (1s and 0s) is written on the memory several times. This method is considered unacceptable in the healthcare environment by many technicians. The only reason cleaning a device is okay is when the device has never had PHI on it; for example, the gift shop computer or the server used to control HVAC in the facility.
- Purging or degaussing is when exposure to a strong magnetic field is used to purge data from the device.
Destroying a device is when physical destruction is used to render a device useless. For example, you can drive a nail through a hard drive to make sure no one can recover the data that was once on that hard drive.

Learning Legal Best Practices and Documentation

HI001 Objectives:

1.4 Explain and interpret legal best practices, requirements, and documentation.

Waivers of liability, Business Associate Agreements (BAA), and Third-party vendor review agreements (SLA, MOU)

Whether or not it is convenient, HIT technicians must deal with legal issues. You need to make sure you are covered for all possible legal issues, so if any issues come up you will be prepared. Best practices and documentation need to be established for HIT technicians because of the necessity to be prepared for a legal issue. For example, HIT technicians are responsible for having the ability to audit all PHI accessed. With the ability to audit activity in information systems, if someone in the hospital violates HIPAA by viewing a patient’s record they should not, the IS can track who accessed the e-PHI that was violated. As another example, when you depend on a vendor to support the equipment in the lab, a contract with the vendor is needed to know the time frame the vendor has to reply to repair needs. If the vendor is slow to respond to your repair requests, you have the contract to remind the vendor of its agreements with consequences to not meeting the commitments outlined.

Hospitals and healthcare providers must use legal best practices to protect themselves from unwarranted lawsuits. Waivers of liability are forms used by healthcare entities to be protected from being inaccurately responsible or sued for harm or debt. An example of a waiver of liability relates to Medicare. Medicare has a law that states healthcare providers are only responsible for providing services that are reasonable and necessary for a patient’s health. However if a patient wants further healthcare, the patient can sign a waiver of liability to receive services not covered by Medicare if he agrees to pay out-of-pocket for the expense of the extra services.
HIPAA requires that when a covered entity requires the services of a person, company, or organization outside the organization, the covered entity must enter into contracts with these third parties. The purpose of this *business associate agreement (BAA)* is to establish rules for safeguarding e-PHI. Third parties need access to e-PHI to fulfill obligations to a covered entity. For example, a vendor needs access to data that might contain e-PHI to research a bug that needs to be fixed with the next update to an IS.

Access allowed to business associates must be limited to the minimum amount of access required to perform necessary functions and activities of the job. This access is controlled by role-based access. This access must have the ability to be audited for activity of the business associates, the same as how auditing abilities are required for internal e-PHI activity.

For example, third parties need a BAA to access e-PHI data to perform the following functions:

- Insurance claims processing
- Data analysis
- Quality assurance
- Private practice office management

Covered entities often require third-party assistance with operations; for example, a software vendor might be contracted to support software and provide regular updates and bug fixes. It is recommended to have a *service-level agreement (SLA)*. An SLA, much like a BAA, establishes how information is to be shared and used. It also sets expectations for service provided so everyone is on the same page and understanding.
In the previous example, a covered entity might use an IS vendor to support that IS and provide updates for bug fixes. The covered entity needs an SLA with the vendor. The SLA establishes the security protocols for the electronic transfer of e-PHI to the company as needed to resolve problems. The SLA also covers the protocol to reset passwords to access the software. The SLA establishes the support protocol, such as if users should call the vendor directly when an issue arises or if the users at a covered entity must go through the IT department to receive support from the vendor.

However, sometimes covered entities need to ensure that personnel and departments within their facility understand the rules regarding access to sensitive information. A memorandum of understanding (MOU) establishes a mutual understanding with personnel or departments that wouldn’t normally have access to sensitive information. For example, cafeteria workers might see PHI occasionally as they prepare meals for patients with special dietary needs. An MOU is needed to make sure the cafeteria workers understand the HIPAA rules about patient privacy.

**memorandum of understanding (MOU)**—Contracts are sometimes necessary within an organization between departments or personnel for mutual understanding of the safeguards of e-PHI.

**HIT in the Real World**

Even though healthcare IT technicians are not healthcare providers, we still are exposed to PHI. We are exposed to PHI even when working remotely. Actually, HIT technicians often have god-like access to data in a hospital because we must have the capability to troubleshoot all systems at any given time. For example, when you troubleshoot problems in the information systems at a hospital, you often encounter problems that require you to ask for a patient’s name, MRN, procedure ordered, or test results. All this information is protected by HIPAA. HIPAA enables healthcare IT technicians to access this information as long as you use the information only in the performance of your job duties.

Having family members in the medical field, I was already familiar with HIPAA and how privately patient information should be respected. When I started my job in the healthcare entity, I was required to complete a short HIPAA study course, pass a test to verify I had read the information, and sign contracts that I would not divulge PHI outside of necessary work duties. Even though I knew the rules, I was still surprised at how many times I needed to obtain patient data while working.

In one specific case, I was troubleshooting the perioperative IS at a facility in Georgia. A nurse was explaining to me that a printed report was not showing information about
patients that should have been on the printed document, and we couldn’t quite com-
municate properly on the phone what she was talking about. So the nurse faxed to
me the printed document with a note written showing what she was trying to explain.
I remember I was pleased with my colleague because she had taken the time to black
out as much PHI as she could and still allow me to see the information I needed to do
my job. Even though she knew that I was privileged to the information, she couldn’t fax
that much information and risk hitting the wrong number on the fax machine and hav-
ing it go to the wrong person.

It’s these careful efforts that we make in our daily jobs that prove we are honorable
professionals who take e-PHI seriously. People notice and appreciate these efforts. It’s
worth it to do your best to honor your obligations even if you are not noticed by some-
one who might reward your efforts.
Chapter Summary

Identifying Standard Agencies, Laws, and Regulations

- Covered entities are health plans, health clearinghouses, and healthcare providers.
- The U.S. Department of Health and Human Services (HHS) is tasked with protecting the health of Americans and providing a means to access healthcare by Americans who are least able to help themselves, containing and treating any national health emergencies, and testing and regulating food and drug supplies.
- The Centers for Medicare & Medicaid Services (CMS) is responsible for administrating Medicare and Medicaid, as well as regulating standards of electronic transactions of claims, provider, and diagnostic codes.
- Version 5010 is the most recent standard format for electronic claims transactions.
- ICD-10 is the most recent standard format for electronic provider and diagnostic codes.
- The Office of the National Coordinator for HIT (ONC) is responsible for certifying EMR/EHR solutions as HIPAA-compliant.
- The National Institute of Standards and Technology (NIST) advances HIT security and usefulness of remote healthcare.
- Medicare is a social insurance program to provide hospital and medical care for elderly and certain disabled citizens.
- Medicaid is a social welfare program to provide health and medical services for certain citizens and families with low incomes and few resources. Medicaid participation by states is voluntary. Medicaid is administrated by states.
- Health Insurance Portability and Accountability Act (HIPAA) is a set of rules for protecting e-PHI (electronic protected health information).
- The Office of Civil Rights (OCR) enforces the HIPAA rules.
- HIPAA has four primary rules: Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule.
- The American Recovery and Reinvestment Act (ARRA), called the Recovery Act, aims to help citizens through the economic recession. In healthcare, the Recovery Act provides funding to HHS branches to help preserve and improve affordable healthcare in the United States.
The Health Information Technology for Economic and Clinical Health (HITECH) Act creates incentive and opportunity for the advancement of HIT through the ONC.

- Meaningful use is the demonstration by healthcare entities to use HIT in a meaningful way.
- Participants in the incentive programs are called eligible providers.

Learning HIPAA Controls and Compliance Issues

- HIPAA aims to ensure confidentiality, integrity, and availability of e-PHI.
- In the event of a violation, or breach, of HIPAA rules, fines may be imposed by the OCR.
- Covered entities are required to ensure confidentiality, integrity, and availability of e-PHI they create, receive, maintain, or transmit; identify and address risks to e-PHI; and ensure compliance by their workforce.
- Written permission must be obtained before e-PHI may be released or distributed to anyone HIPAA does not allow.
- Covered entities must use role-based access control to restrict access to e-PHI by its personnel.

Learning Rules of Record Retention and Disposal

- The three types of health records are public, private, and legal.
- The public health record is used for the collection of public health data to be analyzed by researchers.
- The private health record is the health record created and maintained by an individual.
- The legal health record is collected and retained for use by the patient or legal services.
- Health records must be retained for a minimum of six years. States may add to the length of time for record retention.
- Disposed records must be unreadable, indecipherable, and unable to be reconstructed.
Learning Legal Best Practices and Documentation

- Waivers of liability are forms used by healthcare entities to be protected from being inappropriately responsible for harm or debt.
- Business associate agreements (BAA) are used to ensure a mutual understanding of safeguards of e-PHI between a covered entity and a contracted third party.
- Service-level agreements (SLA) are used to establish how e-PHI is shared and used, as well as expectations of service provided.
- Memoranda of understanding (MOU) are used within a covered entity to ensure understanding of the safeguards of e-PHI among departments or personnel who may not normally be exposed to sensitive information.

Key Terms

- breach notification rule
- business associate agreement (BAA)
- covered entity
- electronic protected health information (e-PHI)
- eligible provider
- enforcement rule
- Health Insurance Portability and Accountability Act (HIPAA)
- healthcare clearinghouse
- ICD 9
- ICD 10
- legal health record
- meaningful use
- memorandum of understanding (MOU)
- privacy rule
- private health record
- public health record
- service-level agreement (SLA)
- Version 5010
- waiver of liability
Acronym Drill

Acronyms sometimes get confusing, especially when a single sentence can have four or five. As an HIT professional, you must know the acronyms and what they stand for. Fill in the blank with the correct acronym for the sentence.

1. The divisions of the _____ involved in healthcare are the _____, the _____, and the _____.
   Answer: __________________________________________________________

2. The new standard of medical diagnosis and inpatient procedure coding, called _____, is required to be adopted by October 1, 2013, by _____-compliant facilities.
   Answer: __________________________________________________________

3. The _____ tests and certifies all _____ solutions to be _____-compliant.
   Answer: __________________________________________________________

4. The _____ enforces _____ rules to protect _____.
   Answer: __________________________________________________________

5. An _____ is used to establish how information is shared and to set expectations for service provided.
   Answer: __________________________________________________________

Review Questions

1. Which branch of the HHS controls the electronic standards of transaction for an insurance claim? And what is the current standard?
   Answer: __________________________________________________________

2. Which HHS division is responsible for enforcing HIPAA rules?
   Answer: __________________________________________________________

3. Do federal or state agencies administrate Medicare? Medicaid?
   Answer: __________________________________________________________

4. What does the HIPAA Enforcement Rule determine?
   Answer: __________________________________________________________
5. What are the goals of the meaningful use of technology in healthcare?
   Answer: ________________________________________________________________
   ________________________________________________________________

6. Why would an eligible provider want to demonstrate the meaningful use of technology?
   Answer: ________________________________________________________________
   ________________________________________________________________

7. What are possible breaches of e-PHI?
   Answer: ________________________________________________________________
   ________________________________________________________________

8. What is the purpose of a public health record?
   Answer: ________________________________________________________________
   ________________________________________________________________

9. What is the basic rule of thumb of record disposal?
   Answer: ________________________________________________________________
   ________________________________________________________________

10. Why are SLAs important and what do they establish?
    Answer: ________________________________________________________________
        ________________________________________________________________

Practical Application

1. The .gov websites are a great resource for HIT professionals. Suppose your boss asks you to develop a contract to be used to establish the SLA with a software vendor to support the software and provide fixes to bugs discovered. Rather than reinventing the wheel by making up your own contract, use an Internet search engine to find templates for contracts and checklists. Find a template on the http://www.hhs.gov website for an SLA/MOU document. Write down the websites where you found the documents.
   Answer: ________________________________________________________________
        ________________________________________________________________
2. Search online for two case examples and resolution agreements to HIPAA violations. You can find several in news articles, and the http://www.hhs.gov website gives some examples where acceptable resolutions agreements were reached. What was the cause of the breach? What were the consequences of the breach? What was the resolution agreement reached? Were policies implemented to prevent the violation from happening again?

Answer: 

_________________________________________________________________
_________________________________________________________________
_________________________________________________________________
_________________________________________________________________

3. While in the waiting room at the free clinic with three other patients, Nurse Jack calls out, “Patti Patient.” Patti Patient begins to walk to Nurse Jack. Before leaving the waiting room, Nurse Jack asks Patti Patient, “Has the herpes cleared up yet?” Is this a HIPAA violation? Why?

Answer: 

_________________________________________________________________
access
  remote, 303-306
  permissions, 283-285
  points (APs), 160
  roles, EHR/EMR, 113-118
account numbers, patients, 32
acknowledgement (ACK) messages, 35, 55
acronyms, 21
Active Directory (AD), 162, 284, 295
active server pages (ASP), 170
acuity, 13
acute care facilities, 6-7, 19
AD (active directory), 162, 284, 295
ADCs (automated dispensing cabinets), 44, 55
add/change billing account (BAR) messages, 35
ad hoc networks, 173-174, 215
administrative offices, hospitals, 8
admissions, 29
admit discharge transfer (ADT) messages, 35, 39-43
admitting physicians, 262, 269
Adobe Flash, 171
ADT (admit discharge transfer) messages, 35, 39-43, 55
adult day care facilities, 7
AES (Advanced Encryption Standard), 176, 302, 313
agencies, governmental. See governmental agencies
algorithms, 297
ambulatory-care facilities, 6
ambulatory/day surgery department, 242
ambulatory surgery centers, 7
American National Standards Institute (ANSI), 34
American Recovery and Reinvestment Act (ARRA), 3, 77, 90
anesthesiologists, 129-130
ANSI (American National Standards Institute), 34
antispyware, 283
APIs (application program interfaces), 171
application service providers (ASPs), 194, 216
applications, dashboards, 38
appointment calendars, HIS (hospital information system), 32
APs (access points), 160
placement, troubleshooting, 190
archiving messages, 37
ARRA (American Recovery and
Reinvestment Act), 3, 77, 90
ASPs (active server pages), 170
ASPs (application service providers),
194, 216
assisted living facilities, 7, 141
organizational structure, 130
asymmetric encryption, 296
attacks, 281
electronic, 282-283
phishing, 282
social engineering, 281
attending physicians, 262, 269
audit trails, 107, 126-127
authentication, 283-284
automated dispensing cabinets
(ADCs), 44, 55

C

CAB (change advisory board), 257
cabling, troubleshooting, 190
cardiovascular department, 242
card scanners, 209
CD (continuity of care document),
260, 269
CCNA (Cisco Certified Network
Associate) certification, 121
CCR (continuity of care record), 260,
269
CCU (critical care unit), 240
CDC (Centers for Disease Control
and Prevention), 68
CDs, 212
Centers for Disease Control and Prevention (CDC), 68
Centers for Medicare & Medicaid Services (CMS), 68-70
change advisory board (CAB), 257
change management, 256-257, 268
chat (Internet), 106
  security, 298
chief complaint, emergency department, 13
ciphers, 297
CIS (clinical information system), 27, 54
Cisco Certified Network Associate (CCNA) certification, 121
classifications, controlled substances, 229
client-server architecture, 153-154
clinical departments (hospitals), 8
clinical information system (CIS), 27, 54
clinical software, 246
  billing and coding, 250-252
  OE (order entry), 248-249
  patient tracking, 247-248
  practice management, 249
  scheduling, 246
  tracking and auditing, 252
cloud computing, 163-165
CMS (Centers for Medicare & Medicaid Services), 68-70, 90
code blue, 230
codes
  current procedural terminology (CPT), 250-252, 268
  evaluation and management (E/M), 250, 268
coding, patients, 133
cold feeds, 43, 55
collaboration sites, security, 298
commands
  ipconfig, 184-185, 216
  ping, 185-186, 216
  tracert, 186-188, 216
communication, 105, 132-133, 139
  security, 298-299
  chat (Internet), 106
  e-mail, 106
  EMR/EHR system, 107
  fax system, 108
  IM (instant messaging), 106
  phone, 109-111
  protocols, 108
  secure FTP, 108-109
  VoIP (Voice over Internet Protocol), 111
compliance (HIPAA), 80-82, 91
CompTIA, 16-17
computed tomography (CT), 9, 234, 266
computerized physician order entries (CPOE), 30, 243, 267
configuration
  peripherals, 198, 216
  workstations, 198-203, 216
consultations, 243
consulting physicians, 262, 269
continuity of care document (CCD), 260, 269
continuity of care record (CCR), 260, 269
controlled substances, 228-229, 266
controls (HIPAA), 91
copiers, security, 289-290
corporate help desks, 25
covered entities, 65, 90
CPOE (computerized physician order entries), 30, 243, 267
CPT (current procedural terminology) codes, 250-252, 268
critical care unit (CCU), 240
crosstalk, troubleshooting, 190
CT (computed tomography), 9, 234, 266
current procedural terminology (CPT) codes, 250-252, 268

D

DAC (discretionary access control), 125
DAs (dental assistants), 116, 140
dashboards, 38
database administrators (DBAs), 122-123, 140
databases, SQL (structured query language), 168
data centers, 286, 311
data encryption standard (DES), 297-298
data flow, 24, 55-56
EDIS ADT, 40-41
EDIS (emergency department information system), 52-53
following, 38-53
HIS-originated ADT, 39-40
ISCIS (clinical information systems), 27

ISHIS (hospital information system), 28-38
LIS (lab IS), 49-51
perioperative IS, 42-43
pharmacy IS, 44-47
radiology IS, 49
RIS (radiology IS), 48-49
support, 25-27
data link layer, Internet, 159-160
day surgery/ambulatory department, 242
DBAs (database administrators), 122-123, 140
DEA (Drug Enforcement Administration), 228
default gateways, 180-181
dental assistants (DAs), 116, 140
Department of Health and Human Services. See HHS (Health and Human Services)
departments, hospitals, 19, 241-242
dermatology, 115
dermatology (DERM) department, 242
DES (data encryption standard), 297-298
desktop support technicians, 123, 140
detailed financial transaction (DFT) message, 35
development environment, 257, 268
devices
mobile computing, 213-217
mobile storage, 217
networks, 175-184
peripheral, 207-211, 217
DFT (detailed financial transaction) messages, 35
DHCP (dynamic host configuration protocol), 179-180, 216
Diagostic laboratories, 49-50
DICOM (digital imaging and communication in medicine), 253-254, 268
dictations, 43
digital imaging and communication in medicine (DICOM), 253-254, 268
discharges, 30
discretionary access control (DAC), 125
disk images, 199
disposal of health records, 85-86, 91
DNS (domain name service), 121, 158-159, 215
document scanners, 208-209
document imaging software, 253-256
documentation
legal, 86-92
semi-structured, 256
structured, 256
unstructured, 256
documents
CCD (continuity of care document), 260, 269
semi-structured, 268
structured, 268
unstructured, 268
domain controllers, 162
domain name service (DNS), 121, 158-159, 215
downtime procedures, 196-197
Drug Enforcement Administration (DEA), 228
duplicate IP address, troubleshooting, 189

DVDs, 212
dynamic host configuration protocol (DHCP), 179-180, 216
dynamic IP addresses, 180

E
ear, nose, throat (ENT) department, 241
ECG (electrocardiogram), 237-238, 266
ED (emergency department), 9, 12-15, 19, 135, 241
EDIS (emergency department information system), 39
ADT data flow, 40-41
data flow, 52-53
EEG (electroencephalogram), 237, 266
EHRs (electronic health records), 3-4, 228, 266
access roles, 113-118
levels of access, 126-127
locally hosted information systems, 193-194
responsibilities, 113-118
role-based access, 124-125
sensitive-patient data access, 126
technical roles, 119-123
third-party access, 123-124
EKG (electrocardiogram), 237-238, 266
electro-magnetic interference (EMI), 190
electroencephalogram (EEG), 237, 266
electronic attacks, 282-283
electronic health records (EHRs). See EHRs (electronic health records)

electronic MAR (eMAR), 44

electronic medical records (EMRs). See EMRs (electronic medical records)

electronic protected health information (e-PHI), 76

eligible providers, 79-80, 91
e-mail, 106

PGP (pretty good privacy), 298

security, 298
eMAR (electronic MAR), 44

emergency department (ED), 9, 12-15, 19, 135, 241

emergency department information system (EDIS). See EDIS (emergency department information system)

E/M (evaluation and management) codes, 250, 268

EMI (electro-magnetic interference), 190

EMRs (electronic medical records), 3-4, 228, 266

access roles, 113-118

levels of access, 126-127

locally hosted information systems, 193-194

responsibilities, 113-118

role-based access, 124-125

sensitive-patient data access, 126

technical roles, 119-123

third-party access, 123-124

EMR/EHR system, 107

encryption, 296-298, 312

AES (Advanced Encryption Standard), 302

asymmetric, 296

DES (data encryption standard), 297-298

PGP (pretty good privacy), 298

symmetric, 296

3DES (triple data encryption standard), 297-298

WEP (wired equivalent privacy), 302

WPA (Wi-Fi Protected Access), 302

WPA2 (Wi-Fi Protected Access 2), 302

Enforcement Rule (HIPAA), 76

ENT (ear, nose, throat) department, 241

environmental security, 293-294

e-PHI (electronic protected health information), 76, 80, 252, 268

security, 299

e-prescribing software, 248-249, 263, 267

ERs (emergency rooms), 241

evaluation and management (E/M) codes, 250, 268

examination rooms, 135

examinations, 243

eXtensible Markup Language (XML), 170

external hard drives, 211

security, 300

F

facilities (healthcare)

acute care, 6-7

hospitals, 7-15

long-term care, 6-7

fax services, 108

security, 299
FDA (Food and Drug Administration), 68
fetal monitors, 134
fiber-optic cabling, 150
File Transfer Protocol (FTP), 108, 139, 153-154, 215
    security, 108-109, 298
filtering messages, 37
fines, HIPAA violations, 80-81
fire monitors, 293
Firewire, 202-203
Flash (Adobe), 171
flash drives, 211
    security, 299
float rooms, 135
Food and Drug Administration (FDA), 68
forwarding messages, 37
FTP (File Transfer Protocol), 108, 139, 153-154, 215
    security, 108-109, 298
full access permissions, 284, 310

Gastroenterology, 129-130
general acute care hospitals, 7
GIF (graphics interchange format)
    files, 253-254, 268
glucose monitors, 236, 266
goals, HIT (Healthcare IT), 15-18
governance board, 257
governmental agencies, 65-71
    healthcare programs
        Medicaid, 75
        Medicare, 74

HHS (Health and Human Services), 66-67
    CMS (Centers for Medicare & Medicaid Services), 68-70
    NIST (National Institute of Standards and Technology), 72-74
    OCR (Office of Civil Rights), 72, 76
    ONC (Office of the National Coordinator for Health Information Technology), 70-71
laws, 76
graphics interchange format (GIF)
    files, 253-254

Hackers, 105
handling PHI, 139
hard drives, external, security, 300
hardware, networks, 175-184, 287-289
Health and Human Services (HHS).
    See HHS (Health and Human Services)
health information exchange (HIE), 25, 54
Health Information Technology for Economic and Clinical Health (HITECH) Act, 3-5, 78-79
Health Insurance Portability and Accountability Act (HIPAA), 65
Health Level 7 (HL7) standard protocol, 34, 55
health records
    disposal, 85-86
    legal, 84-85
    private, 83-84
    public, 83
retention, 85
rules, 91
healthcare clearinghouses, 65-66
healthcare environment, IT functions, 133-134
healthcare facilities
acure care, 6-7
hospitals, 7-15
long-term care, 6-7
Healthcare IT (HIT). See HIT (Healthcare IT)
healthcare programs
Medicaid, 75
Medicare, 74
healthcare providers, 2-3
heating, ventilation, and air conditioning (HVAC) units, 293, 311
help desks, 25, 54
HHS (Health and Human Services), 66-67, 90
CMS (Centers for Medicare & Medicaid Services), 68-70
NIST (National Institute of Standards and Technology), 72-74
OCR (Office of Civil Rights), 72, 76
ONC (Office of the National Coordinator for Health Information Technology), 70-71
HICS (hospital incident command system), 229, 266
HIE (health information exchange), 25, 54
high traffic, servers, 196
HIPAA (Health Insurance Portability and Accountability Act), 65, 90, 97, 280
Breach Notification Rule, 76
compliance, 80-82, 91
controls, 80-82, 91
covered entities, 65
Enforcement Rule, 76
e- PHI (electronic protected health information), 76
ICD-9 codes, 68-70
ICD-10 codes, 68-70
Privacy Rule, 76
record retention and disposal, 83-86
rules, 90
Security Rule, 76
Version 5010, 68-69
HIS (hospital information system), 28-29, 54
appointment calendars, 32
data flow
ADT messages, 39-40
following, 38-53
functions, 29-33
interfaces, 33-38
MPI (master patient index), 32-33
order entries, 30
HIT (healthcare IT), 2-3, 20, 134-138, 148
careers, 16-18
goals, 18
HITECH (Health Information Technology for Economic and Clinical Health) Act, 3-5, 19, 78-79, 91
HL7 formatted messages, 260-262, 269
HL7 (Health Level 7) standard protocol, 34, 55
holding rooms, 135
home health agencies, 7
home healthcare, 141
organization structure, 131
hospices, 132, 141
agencies, 7
organization structure, 131-132
hospital incident command system (HICS), 229, 266
hospital information system (HIS). See HIS (hospital information system)
hospitals, 141
departments, 8, 19, 240-242
  ED (emergency department), 12-15
  inpatient clinics, 9-11
  outpatient clinics, 11
general acute care, 7
HIT technicians, 134-138
medical records offices, 9-10
organization structure, 127-129
patient flow, 9-15
psychiatric, 7
rehabilitation, 7
rooms, 135
hotfixes, 206-207
hot swappable parts, 161
HTML (hypertext markup language), 169
HTTP (Hypertext Transfer Protocol), 153-154, 215
HTTPS (Hypertext Transfer Protocol Secure), 153-154, 215
HVAC (heating, ventilation, and air conditioning) units, 293, 311
hypertext markup language (HTML), 169
hypertext preprocessor (PHP), 170
Hypertext Transfer Protocol (HTTP), 153-154, 215

I-K
IaaS (Infrastructure as a Service), 164-165
ICD-9 codes (HIPAA), 68-70
ICD-10 codes (HIPAA), 68-70, 268
ICU (Intensive Care Unit), 240
IDFs (intermediate distribution frames), 287-288, 311
IE (Internet Explorer), 149
IEEE (Institute of Electrical and Electronics Engineers) 1394, 202-203
imaging, 232-235
document, 253-256
imaging rooms, 135
IM (instant messaging), 106
information system (IS). See IS (information system)
infrastructure
  as a Service (IaaS), 164-165
  networks, 174, 215
inpatient departments, 8, 240-241, 267
  admittance, 9, 19
instant messaging (IM), 106
Intensive Care Unit (ICU), 240
interface engines, 36-38, 55
interfaces, 33, 55, 262-265
  APIs (application program interfaces), 171
dashboards, 38
HIS (hospital information system), 33-38
physician portal, 46
point-to-point connections, 36
interferences, wireless networks, troubleshooting, 190

intermediate distribution frames (IDFs), 287-288, 311

Internet, 149-150

cloud computing, 163-165
data link layer, 159-160
ISPs (Internet service providers), 149
network layer, 156-159
OSI (Open Systems Interconnection) model, 151-152
physical layer, 159-160
protocols, 153-155
routers, 177
servers, 160-163
transport layer, 156-159
virtualization, 166-167

Internet chat, 106

Internet Explorer (IE), 149

Internet Protocol (IP), 157-158, 215

Internet Service Providers (ISPs), 149, 215

intranets, 150, 215

IP addresses, 158
duplicate, troubleshooting, 189
dynamic, 180
static, 179
ipconfig command, 184-185, 216

IP (Internet protocol), 157-158, 215

IS (information system)

CIS (clinical information systems), 27, 54
CPOE (computerized physician order entries), 30, 243

EDIS (emergency department information system), 39
data flow, 52-53
environments, 268

HIS (hospital information system), 28, 54
following data flow, 38-53
functions, 29-33
interfaces, 33-38
MPI (master patient index), 32-33
interfaces, 36

LIS (lab IS), 49-51
messages, 33-35
paths, 36-38

nodes, 263
perioperative, 38-39
pharmacy, 44-47
radiology, 49
RIS (radiology IS), 48-49

ISPs (Internet Service Providers), 149, 215

JPEG (joint photographic experts group) files, 255

key fobs, 290, 291, 311

L

L and D (labor and delivery) department, 240

L2TP (layer 2 tunneling protocol), 305, 313

lab IS (LIS), 49-51

labor and delivery (L &D) department, 240

laboratories, 9, 242
LANs (local area networks), 159
  switches, 182
laptops, power-on passwords, 299
layer 2 tunneling protocol (L2TP), 305, 313
legal health records, 84-85, 91
levels, trauma centers, 231
levels of access, EHR/EMR, 126-127
licensed practical nurses (LPNs), 116, 140
LIS (lab IS), 49-51
load balancing, servers, 196
local area networks (LANs), 159
locally hosted information systems, 193-194
locks, Windows users, 103-104
long-term care facilities, 6-7, 19
lost connectivity, ISPs, troubleshooting, 191
LPNs (licensed practical nurses), 116, 140

MAC (mandatory access control), 124-125
  filtering, 302-303, 313
magnetic resonance imaging (MRI), 9, 235, 266
main distribution frames (MDFs), 287-288, 311
mainframe computers, 160-161
malware, 283, 310
managing
  networks, 216
  resources, 192-197
mandatory access control (MAC), 124-125
  filtering, 302-303, 313
MAR (medication administration record), 44, 55
MAs (medical assistants), 116, 140
master files notification (MFN) messages, 35
master patient index (MPI), 32-33
maximum tolerable downtime (MTD), 306
MDFs (main distribution frames), 287-288, 311
MDs (medical doctors), 114, 139
meaningful use, 79-80, 91
Medicaid, 75, 90
medical assistants (MAs), 116, 140
medical departments, 240-242
medical doctors (MDs), 114, 139
medical imaging, 8, 232-235
medical record numbers (MRNs), 32, 242
medical record offices, 9-10, 19
medical terminology versus technical terminology, 228
medical tests, 236-240
Medicare, 74, 90
medication administration record (MAR), 44, 55
MED/SURG (Medical/Surgical Nursing) department, 241
memorandums of understanding (MOUs), 88, 92
messages, 33-36
  ADT (admit discharge transfer), 39-43, 55
  archiving, 37
filtering, 37
forwarding, 37
HL7 (Health Level 7), 34, 260-262, 269
interface engines, 36-38
ORM, 55
ORU, 55
paths, 36-38
queue management, 37
translating, 37
metadata, 256, 268
MFN (master files notification) messages, 35
mobile computing devices, 213-214, 217
mobile storage, 211-212, 217
modems, 183-184
modify permissions, 284, 310
modules, 246
monitors, troubleshooting, 205
mouse, troubleshooting, 204-205
MOUs (memorandums of understanding), 88, 92
MPI (master patient index), 32-33
MRI (magnetic resonance imaging), 9, 235, 266
MRNs (medical record numbers), 32, 242
MTD (maximum tolerable downtime), 306

N

NAS (network attached storage), 300, 312
national drug code identifier (NDCI), 248-249
National Institute of Standards and Technology (NIST), 72-74, 90
National Institutes of Health (NIH), 68
NAT (network address translation), 177-178
NCID (national drug code identifier), 248-249
neonatal intensive care unit (NICU), 240
network address translation (NAT), 177-178
network administrators, 121, 140
network attached storage (NAS), 300, 312
network layer, Internet, 156-159
networks, 172
ad hoc, 173-174, 215
devices, 175-184
hardware, 175-184, 287-289
infrastructure, 174, 215
managing, 216
NAS (network attached storage), 300
remote access, 303-306
resources, managing, 192-197
secure sockets layer (SSL), 297
security
  electronic attacks, 282-283
  permission levels, 283-285
  phishing, 282
  physical, 286-293
  social engineering, 281
servers, 194-196
tools, 184-188
troubleshooting, 188-192
VPNs (virtual private networks), 17-18, 304
wireless, securing, 302-303, 312-313
NICU (neonatal intensive care unit), 240
NIH (National Institutes of Health), 68
NIST (National Institute of Standards and Technology), 72-74, 90
nodes, 263
NPs (nurse practitioners), 115, 139
nuclear stress tests, 240, 266
NUC (nuclear) department, 242
NUCs (nursing unit clerks), 117, 140
nurse practitioners (NPs), 115, 139
nursing homes, 7, 141
organizational structure, 130
nursing requisitions, 51, 56
nursing unit clerks (NUCs), 117, 140

Office of Civil Rights (OCR), 72, 76, 90
Office of the National Coordinator for Health Information Technology (ONC), 70-71, 90
oncology (ONC) department, 8, 240-241
Open Systems Interconnection (OSI) model, 34
operating divisions (HHS), 67
operating rooms (ORs), 8, 99, 241
operating systems, updates, 203-204
operative records, 43
ophthalmology, 129-130
ophthalmology (OP) department, 242
optical character recognition (OCR) programs, 255-256, 268
order entries, 30
order entry (OE) software, 248-249, 267
order (ORM) messages, 35, 55
organizational structures
assisted living facilities, 130
home healthcare, 131
hospices, 131-132
hospitals, 127-129
nursing homes, 130
private practices, 129-130
surgical centers, 131
ORM (order) messages, 35, 55
ORs (operation rooms), 99, 241
ORU (observation result) messages, 35, 55
OSI (Open Systems Interconnection) model, 34, 151-152
OT (occupational therapy) department, 242
outpatient admittance, 19
outpatient care, 19
outpatient clinics, 8
outpatient departments, 241-242, 267
admittance, 11-15
coding, 133
discharges, 30
registration, 9-10
transfers, 30
PBX (private branch exchange), 109-111
PCPs (primary care physicians), 228, 266
PCTs (patient care technicians), 117, 140
PDF (portable document format) files, 255, 268
pediatrics (PEDS) department, 240-241
penalties, HIPAA violations, 80-81
perioperative IS, 38-39, 55
data flow, 42-43
peripheral devices, 207-211, 217
peripherals, configuring, 198, 216
permission levels, 283-285, 310-311
personal health information (PHI). See PHI (personal health information)
disposing of, 308-309, 314
handling, 139
physical safeguards, 98-103

P

PaaS (Platform as a Service), 164-165
PACS (picture archiving and communication system), 203, 254-255, 268
PACU (post anesthesia care unit), 241
parallel communication, 200-201
PAs (physician assistants), 115, 139
passwords
  best practices, 294-295, 311
  laptops, 299
patches, software, 206-207
pathology, 9
  laboratories, 49-50
paths, messages, 36-38
patient acuity, 229, 266
patient care technicians (PCTs), 117, 140
patient census, 9-10
  Registration office, 29
patient flow, hospitals, 9-15
patient health information (PHI), 280
patient tracking software, 247-248, 267
patients
  account numbers, 32
  admissions, 29
pharmaceuticals, controlled substances, 228-229, 266
pharmacies, 9
pharmacy IS, 46
data flow, 44-47
PET (positron emission tomography), 235, 266
PGP (pretty good privacy), 298, 312
pharmacies, 9
pharmacy IS, 46
data flow, 44-47
PHI (patient health information), 97, 280, 312. See also e-PHI
disposing of, 308-309, 314
handling, 139
physical safeguards, 98-103

PBX (private branch exchange), 109-111
PCPs (primary care physicians), 228, 266
PCTs (patient care technicians), 117, 140
PDF (portable document format) files, 255, 268
pediatrics (PEDS) department, 240-241
penalties, HIPAA violations, 80-81
perioperative IS, 38-39, 55
data flow, 42-43
peripheral devices, 207-211, 217
peripherals, configuring, 198, 216
permission levels, 283-285, 310-311
personal health information (PHI). See PHI (personal health information)
personal health records (PHRs), 84
PET (positron emission tomography), 235, 266
PGP (pretty good privacy), 298, 312
pharmaceuticals, controlled substances, 228-229, 266
pharmacies, 9
pharmacy IS, 46
data flow, 44-47
PHI (patient health information), 97, 280, 312. See also e-PHI
disposing of, 308-309, 314
handling, 139
physical safeguards, 98-103

PBX (private branch exchange), 109-111
PCPs (primary care physicians), 228, 266
PCTs (patient care technicians), 117, 140
PDF (portable document format) files, 255, 268
pediatrics (PEDS) department, 240-241
penalties, HIPAA violations, 80-81
perioperative IS, 38-39, 55
data flow, 42-43
peripheral devices, 207-211, 217
peripherals, configuring, 198, 216
permission levels, 283-285, 310-311
personal health information (PHI). See PHI (personal health information)
personal health records (PHRs), 84
PET (positron emission tomography), 235, 266
PGP (pretty good privacy), 298, 312
pharmaceuticals, controlled substances, 228-229, 266
pharmacies, 9
pharmacy IS, 46
data flow, 44-47
PHI (patient health information), 97, 280, 312. See also e-PHI
disposing of, 308-309, 314
handling, 139
physical safeguards, 98-103
security, 301
technical safeguards, 103-105
phishing, 282, 310
phone switches, 109-110
PHP (hypertext preprocessor), 170
physical layer, Internet, 159-160
physical safeguards, PHI (personal health information), 98-103
physical security, 311
  access, 286-293
  environmental, 293-294
  location, 286-293
physical therapy (PT) department, 241
physician assistants (PAs), 115, 139
physician portals, 46, 56
picture archiving and communication system (PACS), 203, 254-255, 268
ping command, 185-186, 216
plastic surgery department, 241
Platform as a Service (PaaS), 164-165
PMs (practice managers), 117-118, 140
PMs (project managers), 134, 141
point-to-point connections, 36, 55
portable document format (PDF) files, 255, 268
portable X-ray machines, 232-233
port forwarding, 178-179
ports, 156
positron emission tomography (PET), 235, 266
post anesthesia care unit (PACU), 241
postpartum department, 240
power failure, troubleshooting, 191-192
power generators, 294
power problems, troubleshooting, 206
practice management software, 249, 267
practice managers (PMs), 117-118, 140
pretty good privacy (PGP), 298, 312
primary-care facilities, 6
primary-care physicians (PCPs), 228, 262, 266, 269
print servers, 163
printers
  security, 289-290
  troubleshooting, 205-206
Privacy Rule (HIPAA), 76
privacy screens, 100
private branch exchange (PBX), 109-111
private health records, 83-84, 91
private practices, 141
  organizational structure, 129-130
procedural rooms, 135
production/live environment, 257, 268
programming languages, 168-171
project managers (PMs), 134, 141
protocols, Internet, 153-155
psychiatric hospitals, 7
psychology department, 241
PT (physical therapy) department, 241
public health records, 83, 91
QA/test environment, 257, 268
queue management messages, 37
radio frequency identification (RFID), 247-248, 267
radiology departments, 8, 242
radiology IS (RIS), data flow, 48-49
RADIUS (Remote Authentication Dial-In User Service), 176, 302, 313
rapid response, 230
RBAC (role-based access control), 124, 141, 284, 310
RDC (remote desktop connection), 303-304, 313
RDP (Remote Desktop Protocol), 153-155, 215
read permissions, 284, 310
records
CCRs (continuity of care records), 260, 269
disposal, 85-86, 91
EHRs (electronic health records), 3-4, 228, 266
access roles, 113-118
levels of access, 126-127
responsibilities, 113-118
role-based access, 124-125
technical roles, 119-123
third-party access, 123-124
EMRs (electronic medical records), 3-4, 228, 266
access roles, 113-118
responsibilities, 113-118
technical roles, 119-123
legal, 84-85
locally hosted information systems, 193-194
MARs (medication administration records), 44
MRNs (medical record numbers), 242
operative, 43
private, 83-84
public, 83
remote information systems, 193-194
retention, 85, 91
Recovery Act, 77, 90
recovery rooms, 135
referrals, 243
referring physicians, 262, 269
registered nurses (RNs), 115, 140
registration, patients, 9-10
Registration office, patient census, 29
regulations
ARRA (American Recovery and Reinvestment Act), 3
HITECH Act, 3-5, 19
regulatory requirements, 64
ARRA (American Recovery and Reinvestment Act), 77
governmental agencies, 65
healthcare, 74-75
HHS (Health and Human Services), 66-76
HIPAA (Health Insurance Portability and Accountability Act), 65
Breach Notification Rule, 76
compliance, 80-82
controls, 80-82
e-PHI (electronic protected health information), 76
Enforcement Rule, 76
role-based access, EHR/EMR, 124-125
role-based access control (RBAC), 124, 141, 284, 310
routers, 177, 216
routing tables, 121

S

SaaS (Software as a Service), 164-165, 216
SAN (storage area network), 301, 312
scanners, 208-209
biometric, 291, 311
security, 289-290
schedules, controlled substances, 229
scheduling software, 246, 267
screensavers, 103-104
SCSI (small computer system interface), 202-203
secure chat, 106
secure digital (SD) cards, 212
Secure FTP, 108-109
secure officers, 106
secure shell (SSH), 305, 313
Secure Shell (SSH) protocol, 109
secured resources, accessing, 290-293
secure sockets layer (SSL), 297, 312
security, 280
administrators, 140
attacks
  electronic, 282-283
  phishing, 282
  social engineering, 281
authentication, 283
authorization methods, 284
backups, 306-307, 313-314
communication, 298-299
encryption, 296-298, 312
HIPAA, 80
mission levels, 283-285
networks, wireless, 312-313
officers, 106
passwords, best practices, 294-295, 311
PHI, 301, 308-309, 314
physical, 311
  access, 286-293
  allocation, 286-293
  environmental, 293-294
remote access, 303-306
risks, servers, 195
storage, 299-301
wireless networks, 302-303
Security Rule (HIPAA), 76
segments, HL7 messages, 262, 269
semi-structured documentation, 256, 268
sensitive-patient data access, 126
sensitivity labels, 126
serial communication, 200-201
servers, 311
  networks, 160-163, 194-196
  security, 286-300
service level agreements (SLAs), 87, 92
Service Set Identifier (SSID), 176, 313
signature pads, 210-211
single sign on (SSO), 104
SLAs (service level agreements), 87, 92
small computer system interface (SCSI), 202-203
smartphones, security, 299
SNOMED-CT (systemized nomenclature of medicine-clinical terms), 256, 268
social engineering attacks, 281, 310
software, 245, 269
  antispyware, 283
  billing and coding, 267
  change control, 256-257
  clinical
    billing and coding, 250-252
    OE (order entry), 248-249
    patient tracking, 247-248
    practice management, 249
    scheduling, 246
    tracking and auditing, 252
document imaging, 253-256
e-PHI, 252, 268
e-prescribing, 267
interfaces, 262-265
malware, 283
OE (order entry) software, 267
patches, 206-207
patient tracking, 267
practice management, 267
scheduling, 267
spyware, 283
support requests, 258-259
time lockout, 104
Software as a Service (SaaS), 164-165, 216
solutions, 28
spam, 282, 310
specimens, 51
sphygmomanometers, 231-232
spyware, 283, 310
SQL (structured query language), 168
SSH (Secure Shell) protocol, 109, 305, 313
SSID (service set identifiers), 176, 215, 313
SSL (secure sockets layer), 297, 312
SSO (single sign on), 104
stat, 16
static IP addresses, 179
storage
  mobile, 211-212
  security, 299-301
storage area network (SAN), 301, 312
storing messages, 37
structured documentation, 256, 268
structured query language (SQL), 168
subnet masks, 180-181
superbills, 250
support requests, 258-259, 268
surgical centers, 141
  organizational structure, 131
surgical masks, 136
surgical summary reports, 43
switches, LANs (local area networks), 182
symmetric encryption, 296
system administrators, 119-121, 140
systemized nomenclature of medicine-clinical terms (SNOMED-CT), 256, 268

T
T-lines, 150
tagged image file format (TIFF) files, 255, 268
tapes, 212
TCP (transmission control protocol), 157, 215
TCP/IP (Transmission Control Protocol/Internet Protocol), 151
TCU (transitional care unit), 241
technical roles, EHR/EMR, 119-123
technical safeguards, PHI (personal health information), 103-105
technical terminology versus medical terminology, 228
temporal key integrity protocol (TKIP), 176
terminal emulators, 305, 313
terminal services, 167-168, 193
tests, 236-240
thick clients, 193
thin clients, 193
third-party access, EHR/EMR, 123-124
third-party software, remote connections, 305
threads, 260-261, 269
TIFF (tagged image file format) files, 255, 268
time lockout, software, 104
TKIP (temporal key integrity protocol), 176
tools, networks, 184-188
tracert command, 186-188, 216
tracking and auditing software, 252
tracking boards, 12-13
transfers, patients, 30
transitional care unit (TCU), 241
translating messages, 37
Transmission Control Protocol (TCP), 157, 215
transport layer, Internet, 156-159
trauma centers, levels, 231
triage, 13
triple data encryption standard (3DES), 297-298, 312
troubleshooting
monitors, 205
mouse, 204-205
networks, 188-192
power problems, 206
printers, 205-206

U
UAs (unit assistants), 117, 140
ultrasounds, 233, 266
uninterrupted power supply (UPS), 102
unit assistants (UAs), 117, 140
Universal Serial Bus (USB), 201-203, 216
unstructured documentation, 256
unstructured documents, 268
updates, 206-207
updating operating systems, 203-204
UPS (uninterrupted power supply), 102
USB (Universal Serial Bus), 201-203, 216
user test environment, 257, 268

V
vascular stress tests, 238, 266
Version 5010 (HIPAA), 68-69, 90
violations, HIPAA, 80
virtualization, 166-167
virtual private networks (VPNs), 17-18, 304, 313
virus definitions, 200
vitals cuffs, 231-232, 266
Voice over Internet Protocol (VoIP), 111, 139
VoIP phones, security, 299
VPNs (virtual private networks), 17, 18, 304, 313

W-Z
waivers of liability, 86-87
WANs (wide area networks), 149
WAP (wireless access point), 160, 175-177, 215
WAP2 (Wi-Fi Protected Access 2), 215
web browsers, 149
WEP (Wired Equivalent Privacy), 175-176, 302, 312
wide area networks (WANs), 149
Wi-Fi (Wireless Fidelity), 159-160, 215
Wi-Fi Protected Access (WPA), 176, 302, 313
Wi-Fi Protected Access 2 (WPA2), 176, 215, 302, 313
Wired Equivalent Privacy (WEP), 175-176, 302, 312
wireless access point (WAP), 160, 175-177, 215
Wireless Fidelity (Wi-Fi), 159-160, 215
wireless networks, security, 302-303, 312-313
workstations, configuring, 198-203, 216
World Wide Web (WWW), 149
WPA (Wi-Fi Protected Access), 176, 302, 313
WPA2 (Wi-Fi Protected Access 2), 176, 215, 302, 313
write permissions, 284, 310
WWW (World Wide Web), 149

XML (eXtensible Markup Language), 170
X-ray machines, 266