JOY DARK
JEAN ANDREWS

AUTHORIZED

Authorized Cert Guide

Learn, prepare, and practice for exam success

- Master every topic on the HIT-001 exam.
- Assess your knowledge and focus your learning.
- Get the practical workplace knowledge you need!

CompTIA

HEALTHCARE IT TECHNICIAN

HIT-001

PEARSON
IT CERTIFICATION

CompTIA® Healthcare IT Technician HIT-001 Authorized Cert Guide

Joy Dark

Jean Andrews, Ph.D.

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA® Healthcare IT Technician HIT-001 Authorized Cert Guide

ISBN-13: 978-0-7897-4929-1
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

Trademarks

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 of Contents

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. Proffessor 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

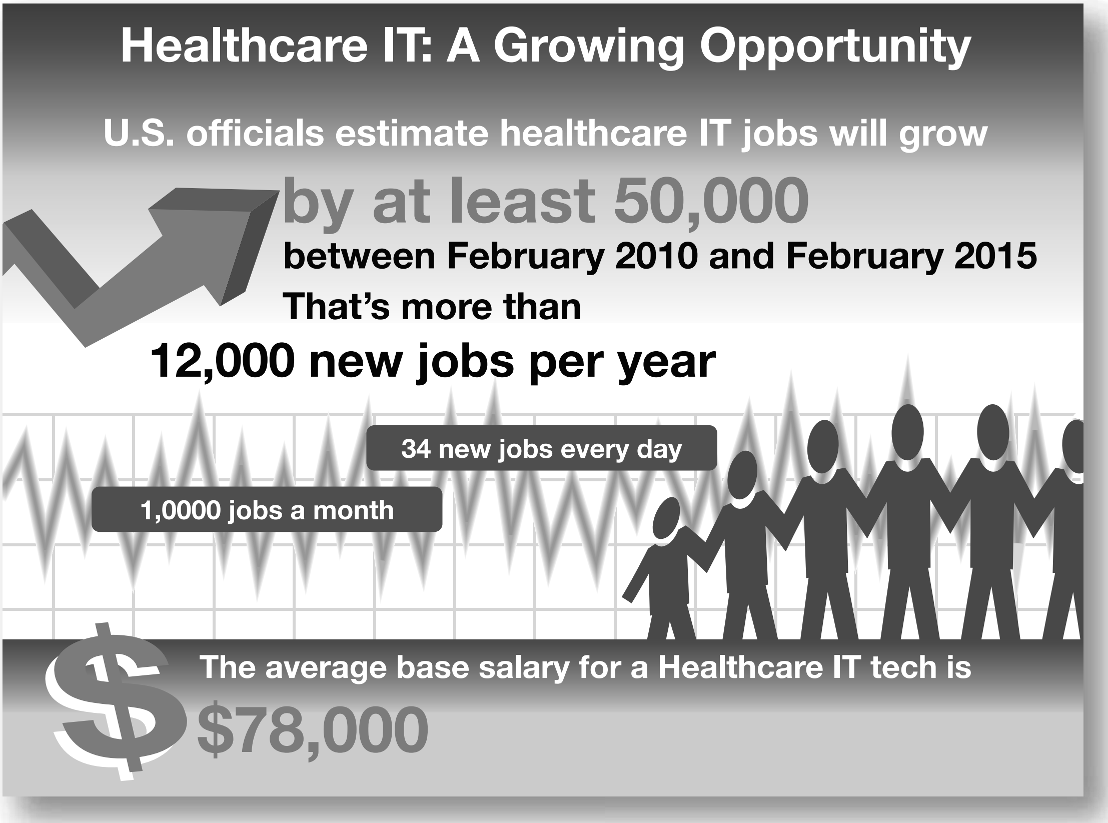
The CompTIA Healthcare Technician specialty certification is a vendor and technology neutral exam designed to ensure IT professionals have the operational, regulatory and security knowledge necessary to provide hardware and software support in medical environments where Electronic Health Record systems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

34 new jobs every day

1,0000 jobs a month

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

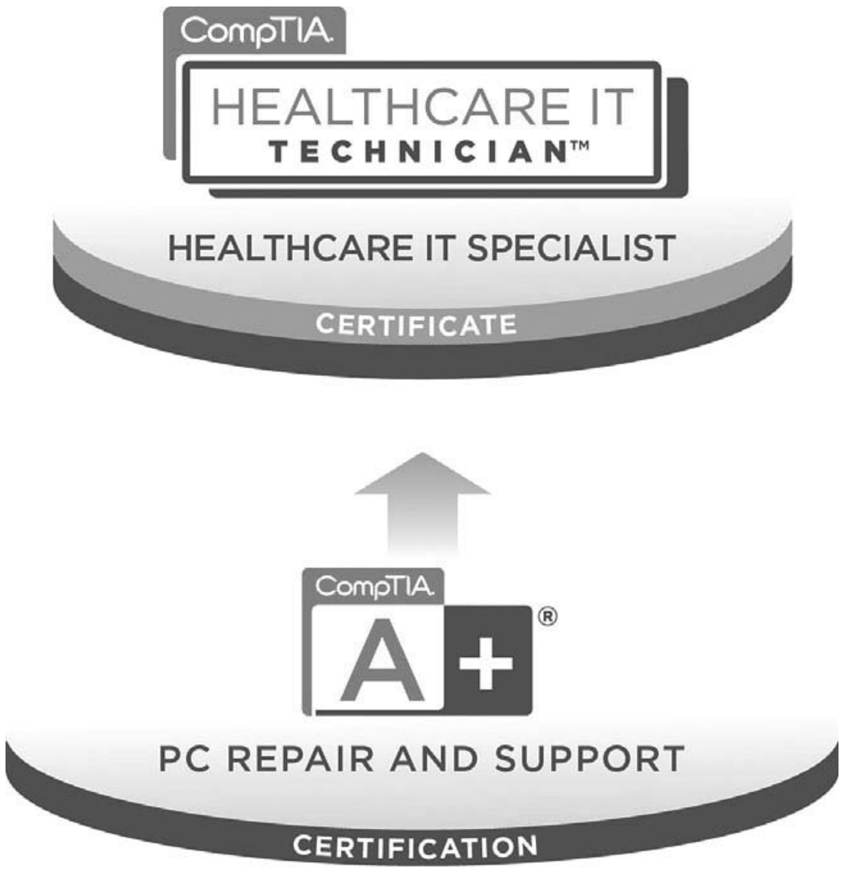
Certifications qualify you for new opportunities, whether locked into a current job, see limited advancement, or need to change careers.

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

Steps to Getting Certified and Staying Certified	
Review Exam Objectives	Review the certification objectives to make sure you know what is covered in the exam: http://certification.comptia.org/Training/testingcenters/examobjectives.aspx
Practice for the Exam	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: http://certification.comptia.org/Training/testingcenters/samplequestions.aspx
Purchase an Exam Voucher	Purchase your exam voucher on the CompTIA Marketplace, which is located at: http://www.comptiastore.com/
Take the Test!	Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: http://certification.comptia.org/Training/testingcenters.aspx

Join the Professional Community

Join IT Pro Community http://itpro.comptia.org	The free IT Pro online community provides valuable content to students and professionals Career IT Job Resources ■ Where to start in IT ■ Career Assessments ■ Salary Trends ■ US Job Board Forums on Networking, Security, Computing and Cutting Edge Technologies Access to blogs written by Industry Experts Current information on Cutting Edge Technologies Access to various industry resource links and articles related to IT and IT careers

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.

CompTIA APPROVED QUALITY CONTENT AUTHORIZED

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—

CompTIA Healthcare IT Technician HIT-001 Official Exam Objectives

Objective	Chapter	Pages
1.0 Regulatory Requirements	3	
1.1 Identify standard agencies, laws, and regulations.	3	65-80
■ HHS	3	65-80
■ ONC	3	65-80
■ CMS	3	65-80
■ HIPAA	3	65-80
■ Medicare	3	65-80
■ Medicaid	3	65-80
■ ARRA	3	65-80
■ HITECH	3	65-80
■ Meaningful use	3	65-80
■ Eligible provider	3	65-80
■ NIST	3	65-80
1.2 Explain and classify HIPAA controls and compliance issues.	3	80-82
■ PHI	3	80-82
■ Covered Entity	3	80-82
■ Security	3	80-82
■ HIPAA Security	3	80-82
■ Violations	3	80-82
■ Fines	3	80-82
■ Requirements	3	80-82
■ Release of information	3	80-82
■ Access permissions	3	80-82
1.3 Summarize regulatory rules of record retention, disposal, and archiving.	3	83-86
■ Documentation requirements	3	83-86
■ Time of storage	3	83-86
■ Types of records	3	83-86
■ Public records	3	83-86
■ Private records	3	83-86
■ Legal health record	3	83-86
■ Methods of record disposal	3	83-86

CompTIA Healthcare IT Technician HIT-001 Official Exam Objectives Continued

Objective	Chapter	Pages
1.4 Explain and interpret legal best practices, requirements, and documentation.	3	86-88
■ Waivers of liability	3	86-88
■ Business Associate Agreements (BAA)	3	86-88
■ Third party vendor review and agreements (SLA, MOU)	3	86-88
2.0 Organizational Behavior	4	
2.1 Use best practices for handling PHI in the workplace.	4	97-105
■ PC placement	4	97-105
■ Privacy screens	4	97-105
■ Printer placement	4	97-105
■ Screensavers	4	97-105
■ Time lockout	4	97-105
2.2 Identify EHR/EMR access roles and responsibilities.	4	113-127
■ Medical roles	4	113-127
■ MD	4	113-127
■ RN	4	113-127
■ PA	4	113-127
■ DA	4	113-127
■ PCT	4	113-127
■ MA	4	113-127
■ NUC	4	113-127
■ UA	4	113-127
■ LPN	4	113-127
■ PM	4	113-127
■ Office Mgr.	4	113-127
■ Staff	4	113-127
■ Technical roles	4	113-127
■ Security administrator	4	113-127
■ Network administrator	4	113-127
■ System administrator	4	113-127

Objective	Chapter	Pages
■ Desktop support	4	113-127
■ Database administrator	4	113-127
■ Business Associate Access and Contractor Access	4	113-127
■ Access limitations based on role and exceptions	4	113-127
■ Emergency access (break the glass)	4	113-127
■ Access based on sensitive patient data	4	113-127
■ Sensitivity labels and clearance	4	113-127
2.3 Apply proper communication methods in the workplace.	4	105-112
■ 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.	4	127-132
■ 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

CompTIA Healthcare IT Technician HIT-001 Official Exam Objectives Continued

Objective	Chapter	Pages
2.5 Given a scenario, execute daily activities while following a code of conduct.	4	132-137
■ Communicate in a professional fashion	4	132-137
■ Adapt procedural behavior according to different situations and environments	4	132-137
■ Imaging room	4	132-137
■ Procedural room	4	132-137
■ Recovery room	4	132-137
■ Examination room	4	132-137
■ Float room	4	132-137
■ Emergency room	4	132-137
■ Adapt social behavior based on sensitivity of the environment	4	132-137
■ Use proper sanitation steps—follow medical precautionary guidelines	4	132-137
■ Conform to requirements set forth by project manager	4	132-137
3.0 IT Operations	5	
3.1 Identify commonly used IT terms and technologies.	5	149-192
■ Protocol terms:	5	149-172
■ TCP/IP	5	149-172
■ DNS	5	149-172
■ DHCP	5	149-172
■ FTP	5	149-172
■ Wireless (802.11x)	5	149-172
■ RDP	5	149-172
■ Devices:	5	149-172
■ Switch	5	172-192
■ Domain controller	5	149-172
■ Printer server	5	149-172
■ Industry terms:	5	149-172
■ ASP	5	149-172
■ ISP	5	149-172
■ Client-server model	5	149-172

Objective	Chapter	Pages
■ Mainframe	5	149-172
■ Cloud Computing	5	149-172
■ Virtualization	5	149-172
■ Terminal services	5	149-172
■ APIs	5	149-172
■ Fiber	5	149-172
■ Languages:	5	149-172
■ XML	5	149-172
■ SQL	5	149-172
■ HTML	5	149-172
■ Flash	5	149-172
■ PHP	5	149-172
■ ASP	5	149-172
3.2 Demonstrate the ability to setup a basic PC workstation within an EHR/EMR environment.	5	198-213
■ Basic installation, configuration and maintenance procedures	5	198-213
■ Basics of operating systems, mouse, keyboard, monitor and applications	5	198-213
3.3 Given a scenario, troubleshoot and solve common PC problems.	5	198-213
■ Malfunctioning hardware	5	198-213
■ Mouse	5	198-213
■ Printer	5	198-213
■ Power	5	198-213
■ Monitor	5	198-213
■ Cables	5	198-213
■ Software patches/hotfixes/updates	5	198-213
■ Documentation	5	198-213
3.4 Install and configure hardware drivers and devices.	5	198-213
■ Imaging devices:	5	198-213
■ Barcode scanner	5	198-213
■ Document scanner	5	198-213
■ Card/badge scanner	5	198-213

CompTIA Healthcare IT Technician HIT-001 Official Exam Objectives Continued

Objective	Chapter	Pages
■ Fax printer	5	198-213
■ Camera	5	198-213
■ Signature pads	5	198-213
■ Physical interfaces:	5	198-213
■ USB	5	198-213
■ IEEE 1394	5	198-213
■ SCSI	5	198-213
■ Serial	5	198-213
■ Bluetooth	5	198-213
■ Mobile storage devices:	5	198-213
■ Flash drives	5	198-213
■ External hard drives	5	198-213
■ DVDs	5	198-213
■ CDs	5	198-213
■ Tapes	5	198-213
■ SD cards	5	198-213
■ Mobile devices:	5	198-213
■ Tablet PCs	5	198-213
■ Smart phones	5	198-213
■ Portable media players	5	198-213
3.5 Compare and contrast basic client networks and tools.	5	172-192
■ 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.	5	172-192
■ Wireless access point	5	172-192
■ Security settings	5	172-192

Objective	Chapter	Pages
■ SSID	5	172-192
■ Guest network	5	172-192
■ Access point placement	5	172-192
■ Router	5	172-192
■ DHCP	5	172-192
■ Port forwarding	5	172-192
■ Internet modem	5	172-192
3.7 Given a scenario, troubleshoot and solve common network problems.	5	172-192
■ Cabling	5	172-192
■ Power	5	172-192
■ IP settings	5	172-192
■ ISP	5	172-192
■ Interference	5	172-192
■ Signal issues	5	172-192
3.8 Explain the features of different backup configurations and the associated maintenance practices.	5	192-197
■ Daily	5	192-197
■ Differential	5	192-197
■ Incremental	5	192-197
■ Archive flags	5	192-197
3.9 Classify different server types, environments, features, and limitations.	5	192-197
■ Database server	5	192-197
■ Application server	5	192-197
■ Interfaces	5	192-197
■ Physical connections	5	192-197
■ Server load and utilization	5	192-197
■ Application services	5	192-197
■ OS and application interoperability	5	192-197
■ Storage space limitations based on application usage and electronic record storage	5	192-197

CompTIA Healthcare IT Technician HIT-001 Official Exam Objectives Continued

Objective	Chapter	Pages
3.10 Compare and contrast EHR/EMR technologies and how each is implemented.	5	192-197
■ ASP/Cloud vs. client-server (locally-hosted)	5	192-197
■ Browser vs. installed application vs. terminal/remote access	5	192-197
■ Hardware requirements	5	192-197
4.0 Medical Business Operations	6	
4.1 Identify commonly used medical terms and devices.	6	227-264
■ Interfaces:	6	245-264
■ HL7	6	259-264
■ e-prescribing	6	245-259
■ CCD	6	259-264
■ CCR	6	259-264
■ ICD10	6	245-259
■ CPT	6	245-259
■ SNOMED	6	245-259
■ NDCID	6	245-259
■ PACS	6	245-259
■ E/M codes	6	245-259
■ Devices:	6	227-244
■ Portable x-ray machine	6	227-244
■ MRI	6	227-244
■ Vitals cuff	6	227-244
■ EKG	6	227-244
■ EEG	6	227-244
■ Ultrasound	6	227-244
■ PET	6	227-244
■ CT	6	227-244
■ Vascular/Nuclear Stress Test	6	227-244
■ Glucose monitor	6	227-244
■ Clinical software and modules:	6	245-259
■ Patient tracking	6	245-259

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

CompTIA Healthcare IT Technician HIT-001 Official Exam Objectives Continued

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.	6	227-244
■ 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.	6	259-264
■ 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

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

CompTIA Healthcare IT Technician HIT-001 Official Exam Objectives Continued

Objective	Chapter	Pages
■ Billing:	6	259-264
■ Improperly formatted patient demographics	6	259-264
■ Improperly formatted superbill	6	259-264
■ Communication link (fax, network, internet)	6	259-264
■ I/O	6	259-264
■ Software configuration settings	6	259-264
4.5 Explain the basics of document imaging.	6	245-259
■ 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.	6	245-259
■ 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.	6	245-259
■ Procedural systematic customization	6	245-259
■ Governance board	6	245-259
■ System patching/updates	6	245-259

Objective	Chapter	Pages
■ Appropriate scheduling	6	245-259
■ Change control environments:	6	245-259
■ evelopment	6	245-259
■ QA/Test	6	245-259
■ User test	6	245-259
■ Production/live	6	245-259
5.0 Security	7	
5.1 Explain physical security controls.	7	285-294
■ 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

CompTIA Healthcare IT Technician HIT-001 Official Exam Objectives Continued

Objective	Chapter	Pages
■ Office hardware	7	285-294
■ Locks	7	285-294
■ Door locks	7	285-294
■ Biometrics	7	285-294
■ Privacy screens	7	285-294
■ UPS	7	285-294
5.2 Summarize the different encryption types and when each is used.	7	296-301
■ Types:	7	296-301
■ SSL	7	296-301
■ DES	7	296-301
■ AES	7	296-301
■ 3DES	7	296-301
■ PGP	7	296-301
■ Communication:	7	296-301
■ Email	7	296-301
■ Chat	7	296-301
■ Smart phone	7	296-301
■ Collaboration sites	7	296-301
■ FTP sites	7	296-301
■ Phone	7	296-301
■ VoIP	7	296-301
■ Fax	7	296-301
■ Storage:	7	296-301
■ Flash drives	7	296-301
■ PCs	7	296-301
■ Laptops	7	296-301
■ SD cards	7	296-301
■ External drives	7	296-301
■ Servers	7	296-301

Objective	Chapter	Pages
■ NAS	7	296-301
■ SANS	7	296-301
■ Dissemination of PHI	7	296-301
5.3 Apply best practices when creating and communicating passwords.	7	294-295
■ Communication of passwords	7	294-295
■ Storage of passwords	7	294-295
■ Password strength (complexity/length)	7	294-295
■ Password reuse	7	294-295
5.4 Classify permission levels based on roles.	7	283-285
■ Read	7	283-285
■ Write	7	283-285
■ Modify	7	283-285
■ Full access	7	283-285
5.5 Identify different remote access methods and security controls.	7	303-306
■ RDC	7	303-306
■ VPN	7	303-306
■ Remote control applications	7	303-306
■ Terminal emulation	7	303-306
■ L2TP	7	303-306
■ SSH	7	303-306
■ HTTPS	7	303-306
■ SFTP	7	303-306
5.6 Recognize wireless security protocols and best practices.	7	302-303
■ WEP	7	302-303
■ WPA	7	302-303
■ WPA2	7	302-303
■ AES	7	302-303
■ RADIUS	7	302-303
■ SSID naming	7	302-303
■ MAC filtering	7	302-303

CompTIA Healthcare IT Technician HIT-001 Official Exam Objectives Continued

Objective	Chapter	Pages
■ Site surveys	7	302-303
■ Access point placement	7	302-303
5.7 Implement best practices in secure disposal of electronic or physical PHI.	7	307-308
■ Secure shredding	7	307-308
■ Degaussing	7	307-308
■ Sanitizing	7	307-308
5.8 Implement backup procedures based on disaster recovery policies.	7	306-307
■ Deployment, configuration and testing of backups	7	306-307
■ Backup storage:	7	306-307
■ Offsite	7	306-307
■ Courier	7	306-307
■ Onsite	7	306-307
■ Methods of secure transfer	7	306-307
■ Backup inventory	7	306-307
5.9 Identify common security risks and their prevention methods.	7	281-283
■ Social engineering—User training	7	281-283
■ Phishing—User training	7	281-283
■ Spamming—Filters	7	281-283
■ Malware—Access control	7	281-283
■ Spyware—Anti-spyware	7	281-283

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 I-1 CompTIA Healthcare IT Technician Exam Topics

Chapter	Exam Topic	CompTIA Healthcare IT Technician Exam Objectives Covered
1	Overview of the HITECH Act, healthcare, and healthcare IT.	Applies to the entire exam.
2	Overview of data flow used in healthcare information systems.	Applies to the entire exam.

Table I-1 Continued

Chapter	Exam Topic	CompTIA Healthcare IT Technician Exam Objectives Covered
3	Identify standard agencies, laws, and regulations. Explain and classify HIPAA controls and compliance issues. Summarize regulatory rules of record retention, disposal, and archiving. Explain and interpret legal best practices, requirements, and documentation.	Objectives 1.1, 1.2, 1.3, 1.4
4	Use best practices for handling PHI in the workplace. Identify EHR/EMR access roles and responsibilities. Apply proper communication methods in the workplace. Identify organizational structures and different methods of operation. Given a scenario, execute daily activities while following a code of conduct.	Objective 2.1, 2.2, 2.3, 2.4, 2.5
5	Identify commonly used IT terms and technologies. Demonstrate the ability to set up a basic PC workstation within an EHR/EMR environment. Given a scenario, troubleshoot and solve common PC problems. Install and configure hardware drivers and devices. Compare and contrast basic client networks and tools. Set up basic network devices and apply basic configuration settings. Given a scenario, troubleshoot and solve common network problems. Explain the features of different backup configurations and the associated maintenance practices. Classify different server types, environments, features, and limitations. Compare and contrast EHR/EMR technologies and how each is implemented.	Objectives 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10

Chapter	Exam Topic	CompTIA Healthcare IT Technician Exam Objectives Covered
6	Identify commonly used medical terms and devices. Explain aspects of a typical clinical environment. Identify and label different components of medical interfaces. Determine common interface problems and escalate when necessary. Explain the basics of document imaging. Given a scenario, determine common clinical software problems. Describe change control best practices and its system-wide effects.	Objectives 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7
7	Explain physical security controls. Summarize the different encryption types and when each is used. Apply best practices when creating and communicating passwords. Classify permission levels based on roles. Identify different remote access methods and security controls. Recognize wireless security protocols and best practices. Implement best practices in secure disposal of electronic or physical PHI. Implement back-sup procedures based on disaster recovery policies. Identify common security risks and their prevention methods.	Objectives 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9

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.

To view the premium edition product page, go to http://www.pearsonitcertification.com/store/product.aspx?isbn=0133104761.

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.

EXAM TIP The Healthcare IT exam focuses on HIPAA quite a bit. Pay close attention to what it is and how it affects IT and healthcare providers.

healthcare clearinghouse—A business that receives healthcare information and translates that information into a standardized format to be sent to a health plan provider. A healthcare clearinghouse is sometimes called a billing service. Basically, a healthcare clearinghouse is a middle person that processes healthcare information.

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)

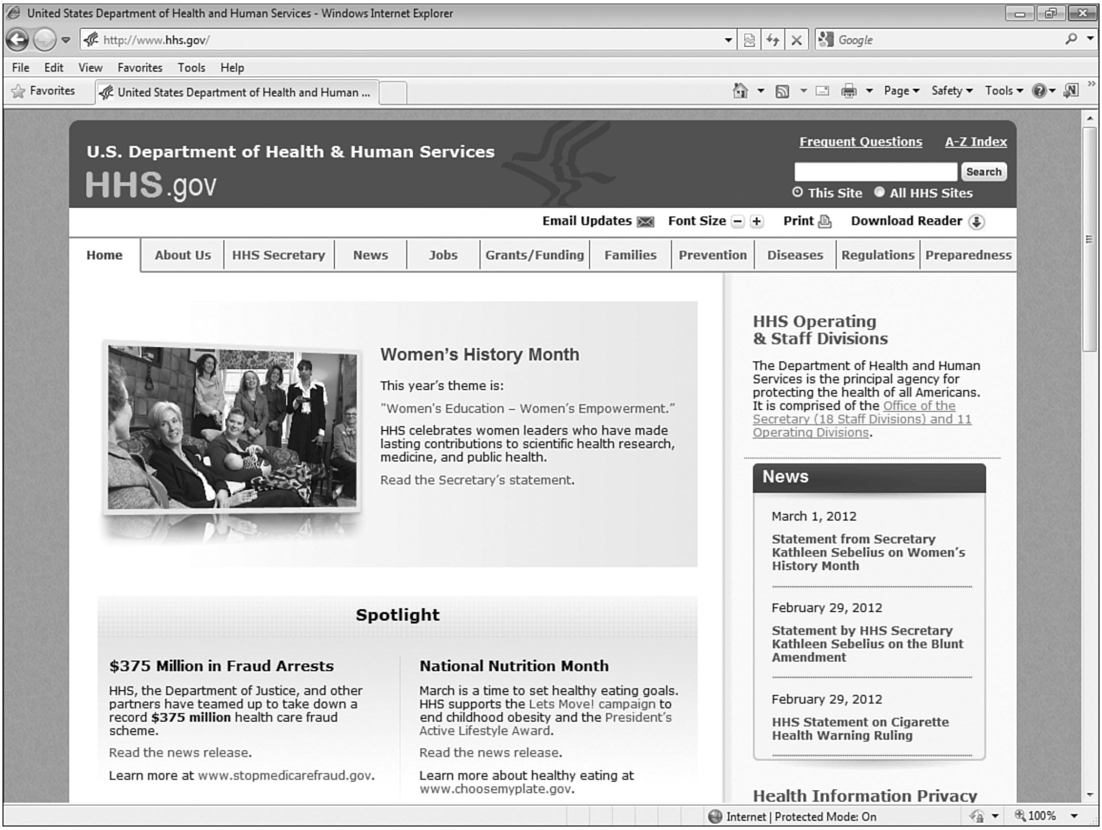
Department of Health and Human Services

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.

EXAM TIP For the Healthcare IT exam, you need to be familiar with the HHS, as well as its operating divisions. Be sure you understand the purpose of the CMS.



Women's History Month

This year's theme is:

"Women's Education – Women's Empowerment."

HHS celebrates women leaders who have made lasting contributions to scientific health research, medicine, and public health.

Read the Secretary's statement.

Spotlight

$375 Million in Fraud Arrests

HHS, the Department of Justice, and other partners have teamed up to take down a record **$375 million** health care fraud scheme.

Read the news release.

Learn more at www.stopmedicarefraud.gov.

National Nutrition Month

March is a time to set healthy eating goals. HHS supports the Lets Move! campaign to end childhood obesity and the President's Active Lifestyle Award.

Read the news release.

Learn more about healthy eating at www.choosemyplate.gov.

HHS Operating & Staff Divisions

The Department of Health and Human Services is the principal agency for protecting the health of all Americans. It is comprised of the Office of the Secretary (18 Staff Divisions) and 11 Operating Divisions.

News

March 1, 2012

Statement from Secretary Kathleen Sebelius on Women's History Month

February 29, 2012

Statement by HHS Secretary Kathleen Sebelius on the Blunt Amendment

February 29, 2012

HHS Statement on Cigarette Health Warning Ruling

Health Information Privacy

Figure 3-1 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

Division	Abbreviation
Administration for Children and Families	ACF
Administration on Children, Youth, and Families	ACYF
Administration on Aging	AoA
Agency for Healthcare Research and Quality	AHRQ

Table 3-1 Continued

Division	Abbreviation
Centers for Disease Control and Prevention	CDC
Centers for Medicare & Medicaid Services	CMS
Food and Drug Administration	FDA
Health Resources and Services Administration	HRSA
Indian Health Service	IHS
National Institutes of Health	NIH
National Cancer Institute	NCI
Office of the Inspector General	OIG
Substance Abuse and Mental Health Services Administration	SAMHSA

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)

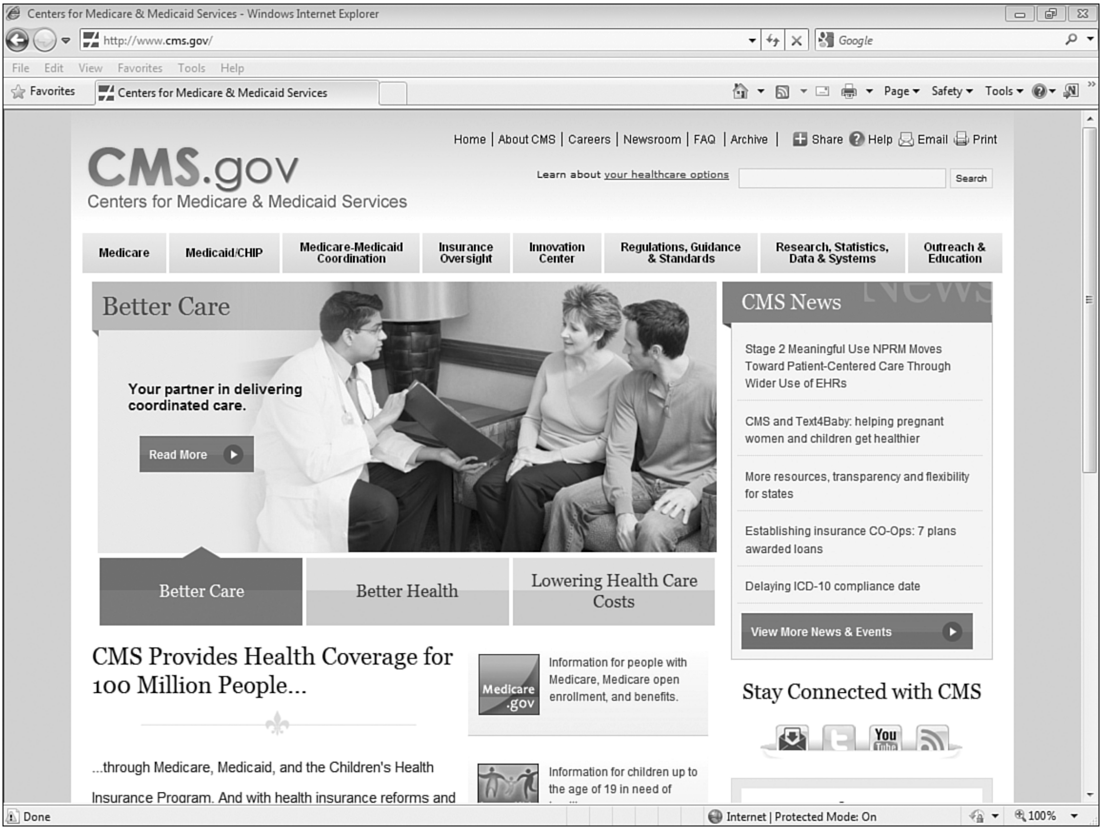
Centers for Medicare & Medicaid Services (CMS)

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.

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.


Centers for Medicare & Medicaid Services - Windows Internet Explorer
http://www.cms.gov/
Google
File Edit View Favorites Tools Help
Favorites
Centers for Medicare & Medicaid Services
Page Safety Tools
Home | About CMS | Careers | Newsroom | FAQ | Archive | Share Help Email Print
CMS.gov
Centers for Medicare & Medicaid Services
Learn about your healthcare options
Search
Medicare
Medicaid/CHIP
Medicare-Medicaid Coordination
Insurance Oversight
Innovation Center
Regulations, Guidance & Standards
Research, Statistics, Data & Systems
Outreach & Education
Better Care
Read More
CMS News
View More News & Events
Better Care
Better Health
Lowering Health Care Costs
Stay Connected with CMS
Medicare .gov
Done
Internet | Protected Mode: On
100%

Your partner in delivering coordinated care.

Stage 2 Meaningful Use NPRM Moves Toward Patient-Centered Care Through Wider Use of EHRs

CMS and Text4Baby: helping pregnant women and children get healthier

More resources, transparency and flexibility for states

Establishing insurance CO-Ops: 7 plans awarded loans

Delaying ICD-10 compliance date

CMS Provides Health Coverage for 100 Million People...

...through Medicare, Medicaid, and the Children's Health Insurance Program. And with health insurance reforms and

Information for people with Medicare, Medicare open enrollment, and benefits.

Information for children up to the age of 19 in need of

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

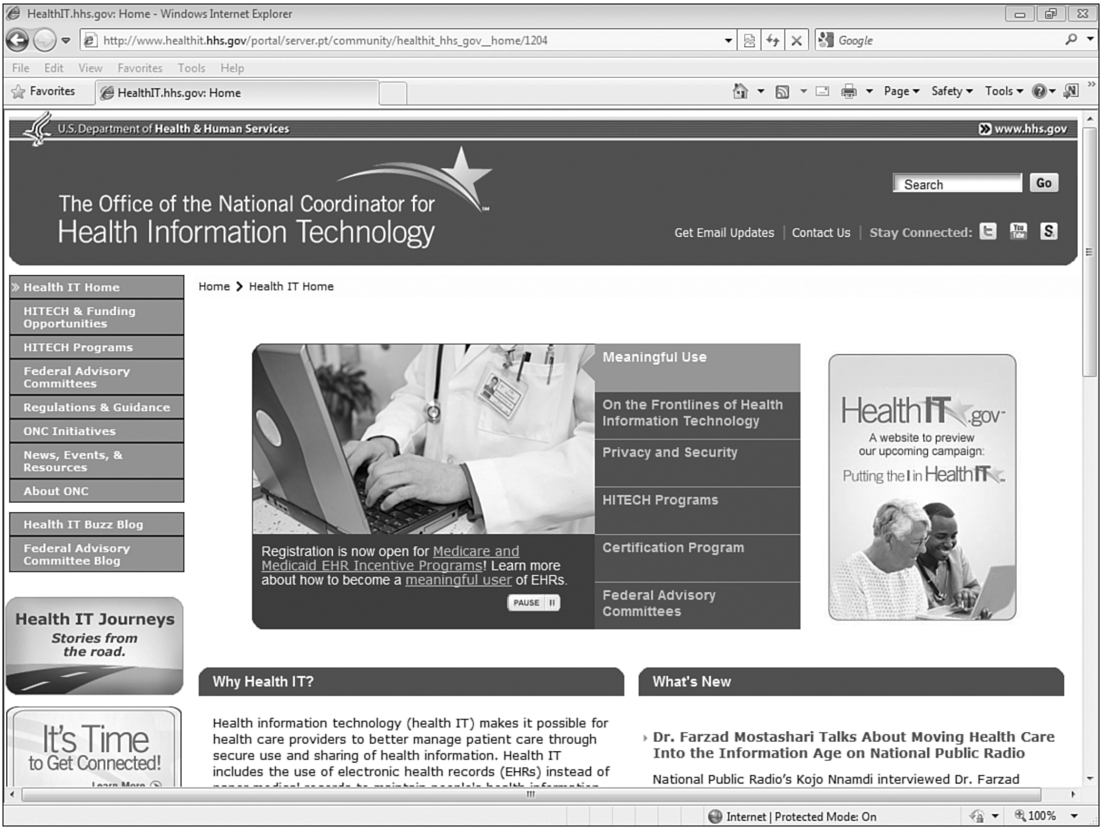
The purpose of coding is to equate expenses in a hospital into numbers. For example, whenever a doctor examines a patient, a nurse uses a syringe to administer a drug, or a patient receives a diagnosis, a code must be generated to represent the expense associated with providing this patient care. When 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.



HealthIT.hhs.gov: Home - Windows Internet Explorer
http://www.healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__home/1204
Google
File Edit View Favorites Tools Help
Favorites
HealthIT.hhs.gov: Home
Page Safety Tools
U.S. Department of Health & Human Services
www.hhs.gov
The Office of the National Coordinator for
Health Information Technology
Search
Go
Get Email Updates | Contact Us | Stay Connected:
Health IT Home
HITECH & Funding Opportunities
HITECH Programs
Federal Advisory Committees
Regulations & Guidance
ONC Initiatives
News, Events, & Resources
About ONC
Health IT Buzz Blog
Federal Advisory Committee Blog
Health IT Journeys
Stories from the road.
It's Time to Get Connected!
Home > Health IT Home
Meaningful Use
On the Frontlines of Health Information Technology
Privacy and Security
HITECH Programs
Certification Program
Federal Advisory Committees
PAUSE
HealthIT.gov
A website to preview our upcoming campaign:
Putting the I in HealthIT
Why Health IT?
What's New
Internet | Protected Mode: On
100%

Registration is now open for Medicare and Medicaid EHR Incentive Programs! Learn more about how to become a meaningful user of EHRs.

Health information technology (health IT) makes it possible for health care providers to better manage patient care through secure use and sharing of health information. Health IT includes the use of electronic health records (EHRs) instead of

Dr. Farzad Mostashari Talks About Moving Health Care Into the Information Age on National Public Radio

National Public Radio's Kojo Nnamdi interviewed Dr. Farzad

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

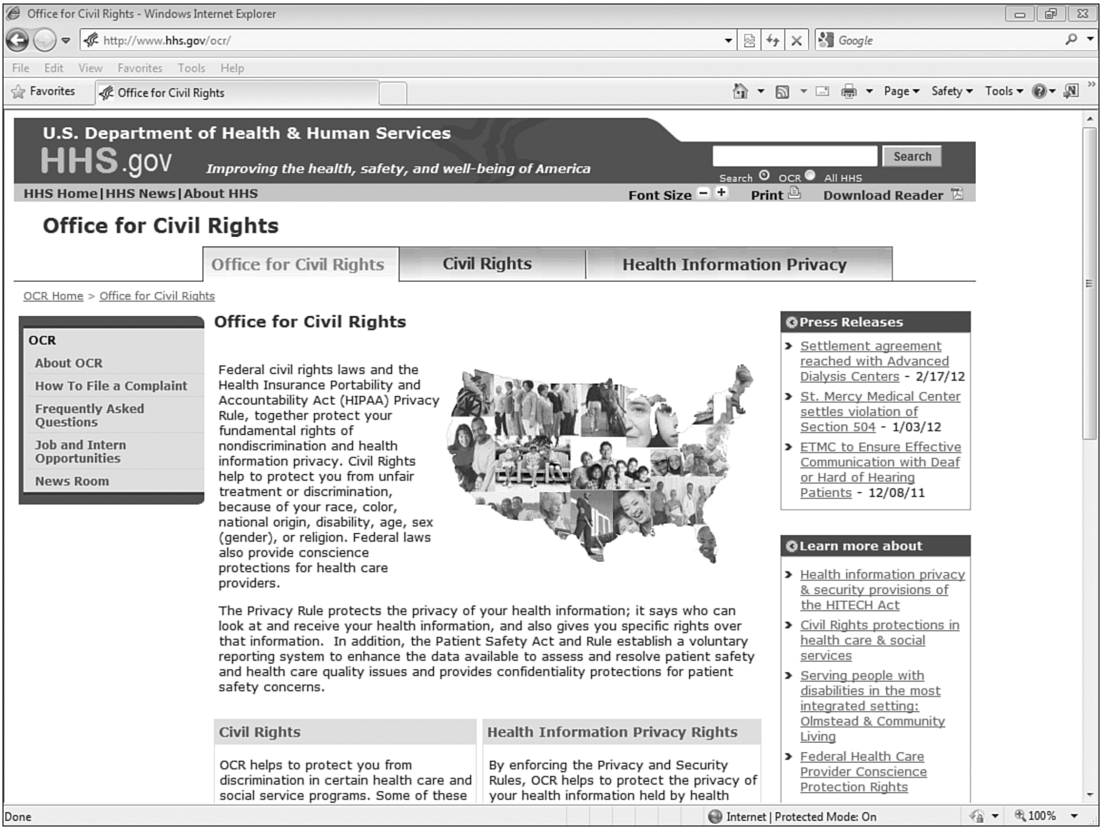
Photo credit: http://www.healthit.hhs.gov

> **EXAM TIP** For the Healthcare IT exam, you need to know about the ONC, what it does, and why it was created.

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.


Office for Civil Rights - Windows Internet Explorer
http://www.hhs.gov/ocr/
Google
File Edit View Favorites Tools Help
Favorites
Office for Civil Rights
Page ▾ Safety ▾ Tools ▾
U.S. Department of Health & Human Services
HHS.gov
Improving the health, safety, and well-being of America
Search
Search ○ OCR ● All HHS
HHS Home | HHS News | About HHS
Font Size − +
Print
Download Reader
Office for Civil Rights
Office for Civil Rights
Civil Rights
Health Information Privacy
OCR Home > Office for Civil Rights
OCR
About OCR
How To File a Complaint
Frequently Asked Questions
Job and Intern Opportunities
News Room
Press Releases
Learn more about
Done
Internet | Protected Mode: On
100%

Office for Civil Rights

Federal civil rights laws and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, together protect your fundamental rights of nondiscrimination and health information privacy. Civil Rights help to protect you from unfair treatment or discrimination, because of your race, color, national origin, disability, age, sex (gender), or religion. Federal laws also provide conscience protections for health care providers.

The Privacy Rule protects the privacy of your health information; it says who can look at and receive your health information, and also gives you specific rights over that information. In addition, the Patient Safety Act and Rule establish a voluntary reporting system to enhance the data available to assess and resolve patient safety and health care quality issues and provides confidentiality protections for patient safety concerns.

Civil Rights

OCR helps to protect you from discrimination in certain health care and social service programs. Some of these

Health Information Privacy Rights

By enforcing the Privacy and Security Rules, OCR helps to protect the privacy of your health information held by health

Press Releases

- Settlement agreement reached with Advanced Dialysis Centers - 2/17/12
- St. Mercy Medical Center settles violation of Section 504 - 1/03/12
- ETMC to Ensure Effective Communication with Deaf or Hard of Hearing Patients - 12/08/11

Learn more about

- Health information privacy & security provisions of the HITECH Act
- Civil Rights protections in health care & social services
- Serving people with disabilities in the most integrated setting: Olmstead & Community Living
- Federal Health Care Provider Conscience Protection Rights

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

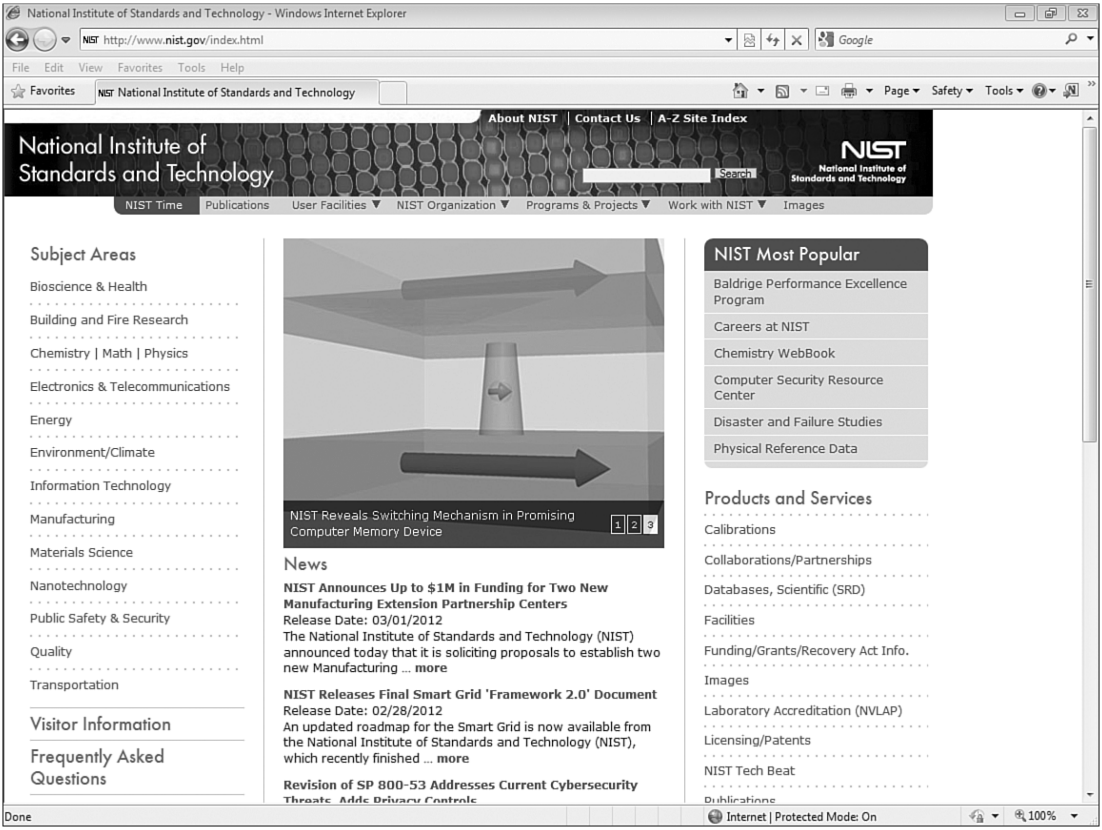
National Institute of Standards and Technology (NIST)

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.


National Institute of Standards and Technology - Windows Internet Explorer
http://www.nist.gov/index.html
Google
File
Edit
View
Favorites
Tools
Help
Favorites
National Institute of Standards and Technology
Page
Safety
Tools
About NIST
Contact Us
A-Z Site Index
National Institute of Standards and Technology
Search
NIST
National Institute of Standards and Technology
NIST Time
Publications
User Facilities
NIST Organization
Programs & Projects
Work with NIST
Images
1
2
3
Done
Internet | Protected Mode: On
100%

Subject Areas

- Bioscience & Health
- Building and Fire Research
- Chemistry | Math | Physics
- Electronics & Telecommunications
- Energy
- Environment/Climate
- Information Technology
- Manufacturing
- Materials Science
- Nanotechnology
- Public Safety & Security
- Quality
- Transportation

Visitor Information

Frequently Asked Questions

NIST Reveals Switching Mechanism in Promising Computer Memory Device

News

NIST Announces Up to $1M in Funding for Two New Manufacturing Extension Partnership Centers
Release Date: 03/01/2012
The National Institute of Standards and Technology (NIST) announced today that it is soliciting proposals to establish two new Manufacturing ... **more**

NIST Releases Final Smart Grid 'Framework 2.0' Document
Release Date: 02/28/2012
An updated roadmap for the Smart Grid is now available from the National Institute of Standards and Technology (NIST), which recently finished ... **more**

Revision of SP 800-53 Addresses Current Cybersecurity Threats, Adds Privacy Controls

NIST Most Popular

- Baldrige Performance Excellence Program
- Careers at NIST
- Chemistry WebBook
- Computer Security Resource Center
- Disaster and Failure Studies
- Physical Reference Data

Products and Services

- Calibrations
- Collaborations/Partnerships
- Databases, Scientific (SRD)
- Facilities
- Funding/Grants/Recovery Act Info.
- Images
- Laboratory Accreditation (NVLAP)
- Licensing/Patents
- NIST Tech Beat
- Publications

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.

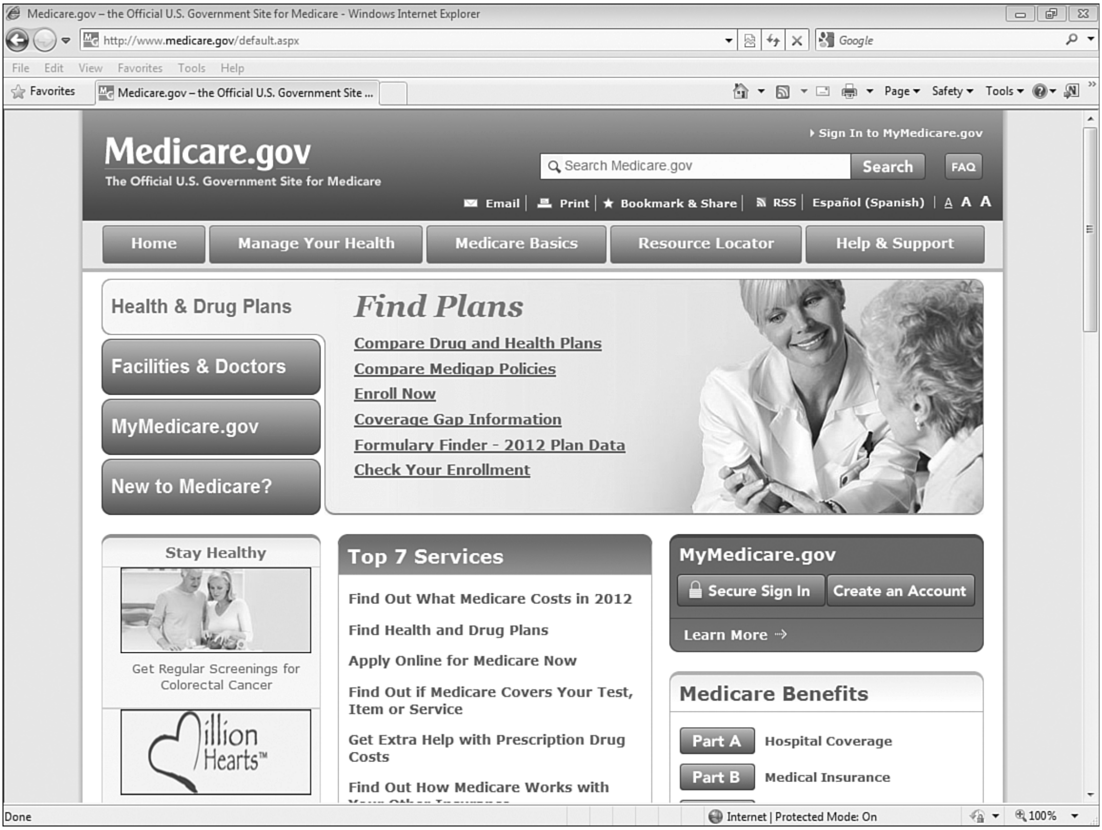
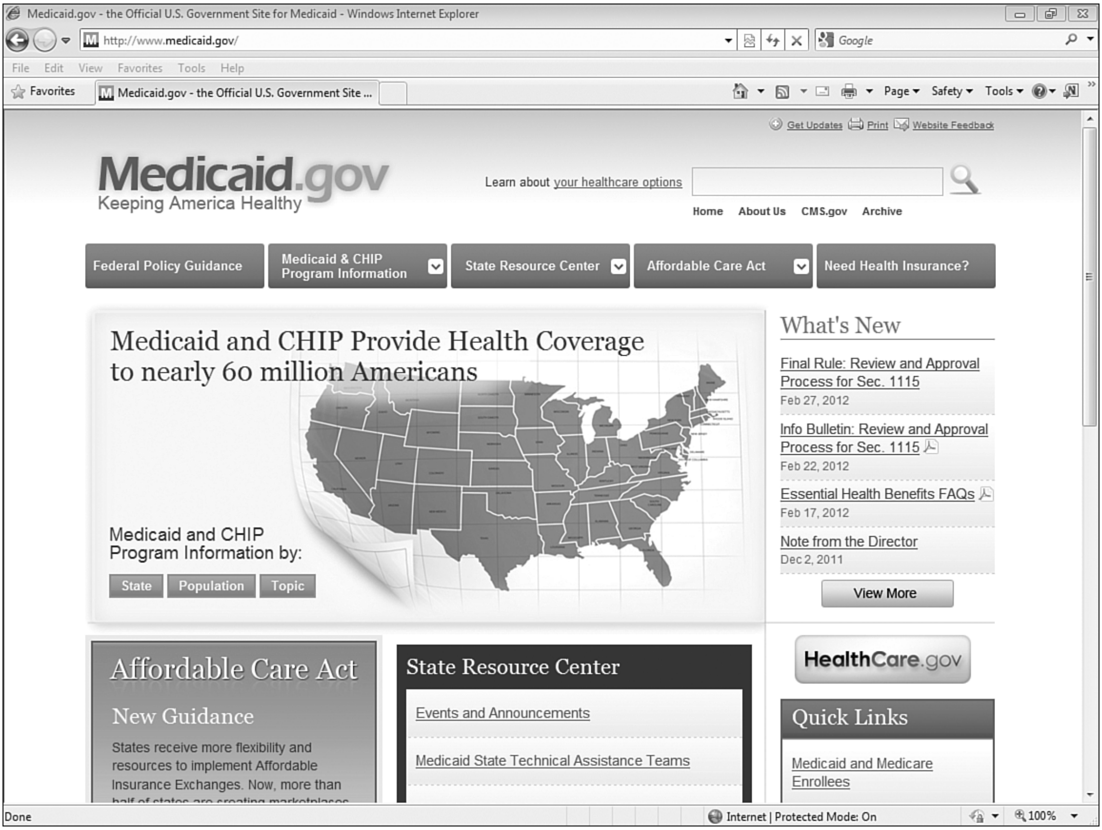

Medicare.gov – the Official U.S. Government Site for Medicare - Windows Internet Explorer
http://www.medicare.gov/default.aspx
Google
File Edit View Favorites Tools Help
Favorites
Medicare.gov – the Official U.S. Government Site ...
Page Safety Tools
Medicare.gov
The Official U.S. Government Site for Medicare
Sign In to MyMedicare.gov
Search Medicare.gov
Search
FAQ
Email
Print
Bookmark & Share
RSS
Español (Spanish)
A A A
Home
Manage Your Health
Medicare Basics
Resource Locator
Help & Support
Health & Drug Plans
Facilities & Doctors
MyMedicare.gov
New to Medicare?
Find Plans
Compare Drug and Health Plans
Compare Medigap Policies
Enroll Now
Coverage Gap Information
Formulary Finder - 2012 Plan Data
Check Your Enrollment
Stay Healthy
Get Regular Screenings for Colorectal Cancer
Million Hearts™
Top 7 Services
Find Out What Medicare Costs in 2012
Find Health and Drug Plans
Apply Online for Medicare Now
Find Out if Medicare Covers Your Test, Item or Service
Get Extra Help with Prescription Drug Costs
Find Out How Medicare Works with
MyMedicare.gov
Secure Sign In
Create an Account
Learn More
Medicare Benefits
Part A Hospital Coverage
Part B Medical Insurance
Done
Internet | Protected Mode: On
100%

Figure 3-6 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

EXAM TIP For the Healthcare IT exam, you need to understand what Medicare and Medicaid are and how funding comes to healthcare providers.

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.


Medicaid.gov - the Official U.S. Government Site for Medicaid - Windows Internet Explorer
http://www.medicaid.gov/
Google
File Edit View Favorites Tools Help
Favorites
Medicaid.gov - the Official U.S. Government Site ...
Page Safety Tools
Get Updates Print Website Feedback
Medicaid.gov
Keeping America Healthy
Learn about your healthcare options
Home About Us CMS.gov Archive
Federal Policy Guidance
Medicaid & CHIP Program Information
State Resource Center
Affordable Care Act
Need Health Insurance?
State Population Topic
View More
HealthCare.gov
Done
Internet | Protected Mode: On
100%

Medicaid and CHIP Provide Health Coverage to nearly 60 million Americans

Medicaid and CHIP Program Information by:

What's New

Final Rule: Review and Approval Process for Sec. 1115
Feb 27, 2012

Info Bulletin: Review and Approval Process for Sec. 1115
Feb 22, 2012

Essential Health Benefits FAQs
Feb 17, 2012

Note from the Director
Dec 2, 2011

Affordable Care Act

New Guidance

States receive more flexibility and resources to implement Affordable Insurance Exchanges. Now, more than half of states are creating marketplaces

State Resource Center

Events and Announcements

Medicaid State Technical Assistance Teams

Quick Links

Medicaid and Medicare Enrollees

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)

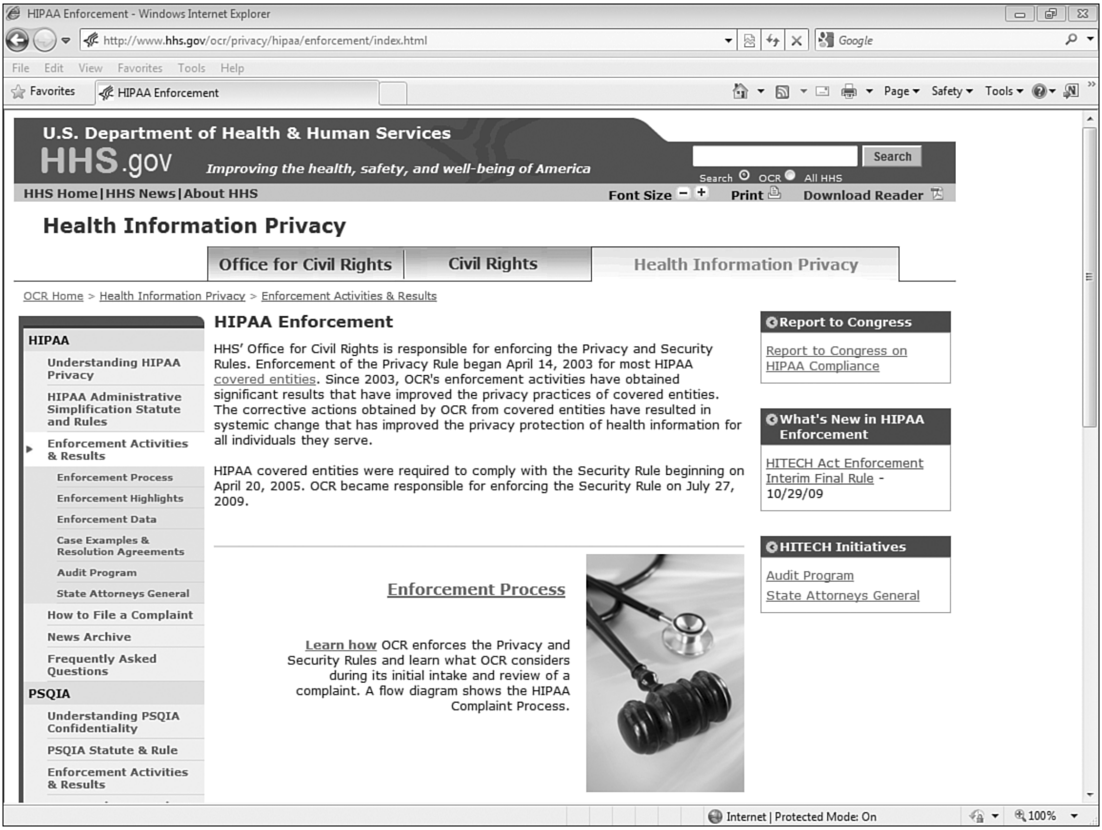
The Health Insurance Portability and Accountability Act (HIPAA)—http://www.hhs.gov/ocr/privacy—was created in 1996 to provide a standard set of rules for all covered entities to follow to protect patient health information and to help healthcare providers transition from paper to electronic health records.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

electronic protected health information (e-PHI)—HIPAA protects the electronic information that can be used to identify an individual. e-PHI is information created, used, or disclosed about a patient while providing healthcare.

- **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.


HIPAA Enforcement - Windows Internet Explorer
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
Google
File Edit View Favorites Tools Help
Favorites
HIPAA Enforcement
Page Safety Tools
U.S. Department of Health & Human Services
HHS.gov
Improving the health, safety, and well-being of America
Search
Search OCR All HHS
HHS Home | HHS News | About HHS
Font Size
Print
Download Reader
Office for Civil Rights
Civil Rights
Health Information Privacy
HIPAA
Understanding HIPAA Privacy
HIPAA Administrative Simplification Statute and Rules
Enforcement Activities & Results
Enforcement Process
Enforcement Highlights
Enforcement Data
Case Examples & Resolution Agreements
Audit Program
State Attorneys General
How to File a Complaint
News Archive
Frequently Asked Questions
PSQIA
Understanding PSQIA Confidentiality
PSQIA Statute & Rule
Enforcement Activities & Results
Internet | Protected Mode: On
100%

Health Information Privacy

OCR Home > Health Information Privacy > Enforcement Activities & Results

HIPAA Enforcement

HHS' Office for Civil Rights is responsible for enforcing the Privacy and Security Rules. Enforcement of the Privacy Rule began April 14, 2003 for most HIPAA covered entities. Since 2003, OCR's enforcement activities have obtained significant results that have improved the privacy practices of covered entities. The corrective actions obtained by OCR from covered entities have resulted in systemic change that has improved the privacy protection of health information for all individuals they serve.

HIPAA covered entities were required to comply with the Security Rule beginning on April 20, 2005. OCR became responsible for enforcing the Security Rule on July 27, 2009.

Enforcement Process

Learn how OCR enforces the Privacy and Security Rules and learn what OCR considers during its initial intake and review of a complaint. A flow diagram shows the HIPAA Complaint Process.

Report to Congress

Report to Congress on HIPAA Compliance

What's New in HIPAA Enforcement

HITECH Act Enforcement Interim Final Rule - 10/29/09

HITECH Initiatives

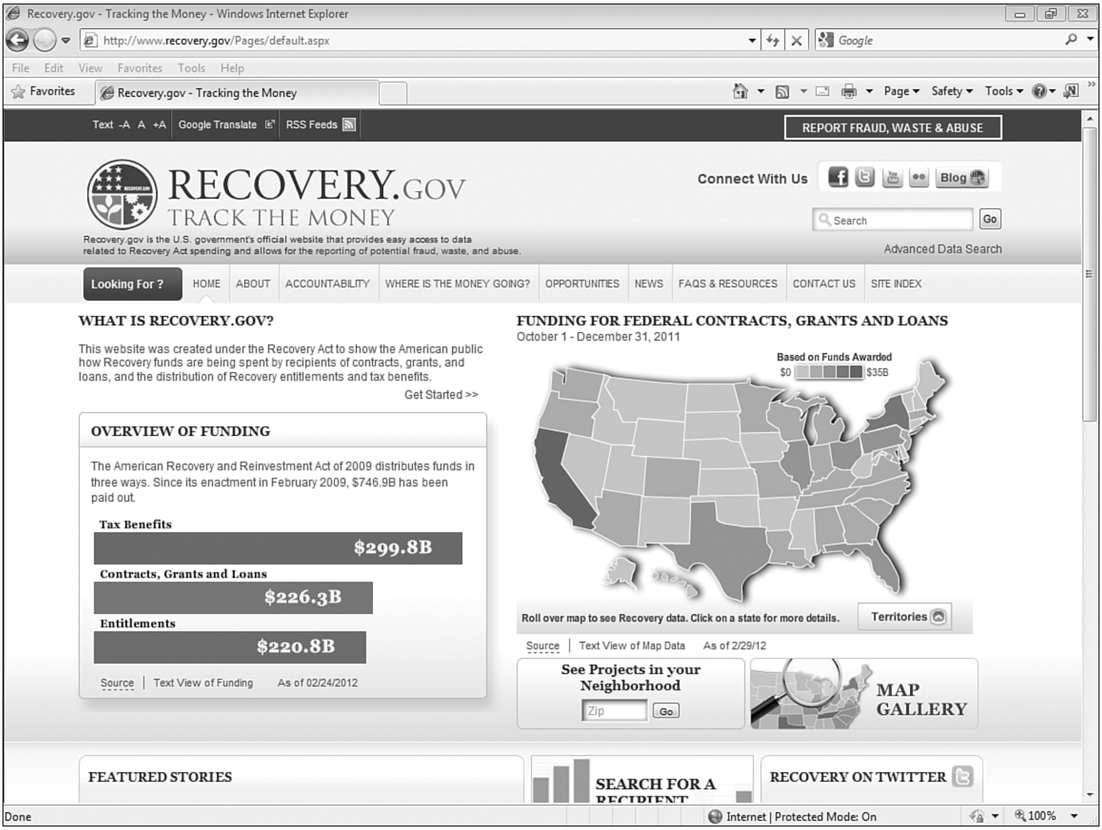
Audit Program
State Attorneys General

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.



Recovery.gov is the U.S. government's official website that provides easy access to data related to Recovery Act spending and allows for the reporting of potential fraud, waste, and abuse.

WHAT IS RECOVERY.GOV?

This website was created under the Recovery Act to show the American public how Recovery funds are being spent by recipients of contracts, grants, and loans, and the distribution of Recovery entitlements and tax benefits.

OVERVIEW OF FUNDING

The American Recovery and Reinvestment Act of 2009 distributes funds in three ways. Since its enactment in February 2009, $746.9B has been paid out.

Tax Benefits	$299.8B
Contracts, Grants and Loans	$226.3B
Entitlements	$220.8B

FUNDING FOR FEDERAL CONTRACTS, GRANTS AND LOANS
October 1 - December 31, 2011

Roll over map to see Recovery data. Click on a state for more details.

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

HI001 Objectives:

1.2 Explain and classify HIPAA controls and compliance issues.

PHI, Covered Entity, Security, HIPAA Security, Violations, Fines, Requirements, Release of information, and Access permissions

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

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

- **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. 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

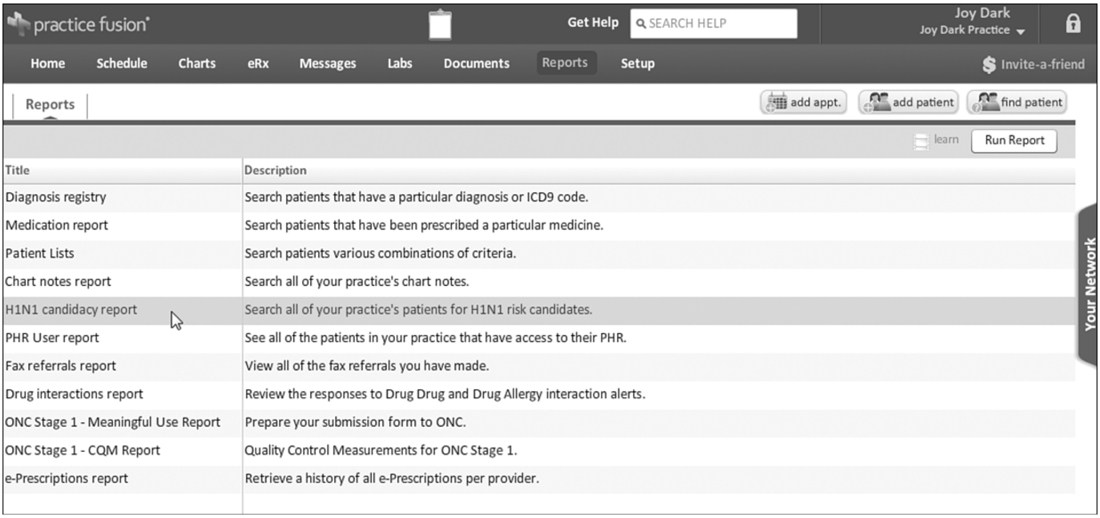
Documentation requirements are defined by HIPAA, but some requirements vary from state to state. The state defines how long records must be kept, called record retention. HIPAA defines how records are disposed of and how they are kept in storage (archived). The three types of records are public, private,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



Title	Description
Diagnosis registry	Search patients that have a particular diagnosis or ICD9 code.
Medication report	Search patients that have been prescribed a particular medicine.
Patient Lists	Search patients various combinations of criteria.
Chart notes report	Search all of your practice's chart notes.
H1N1 candidacy report	Search all of your practice's patients for H1N1 risk candidates.
PHR User report	See all of the patients in your practice that have access to their PHR.
Fax referrals report	View all of the fax referrals you have made.
Drug interactions report	Review the responses to Drug Drug and Drug Allergy interaction alerts.
ONC Stage 1 - Meaningful Use Report	Prepare your submission form to ONC.
ONC Stage 1 - CQM Report	Quality Control Measurements for ONC Stage 1.
e-Prescriptions report	Retrieve a history of all e-Prescriptions per provider.

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.

legal health record—Health organizations must retain a health record of patients for use by the patient or legal services.

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 inappropriately 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.

waiver of liability—A contract used to protect healthcare entities from being inappropriately responsible or sued for harm or debt.

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.

business associate agreement (BAA)—A contract used between healthcare entities and third parties to establish a mutual understanding of safeguards of e-PHI.

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.

service-level agreement (SLA)—Contracts used between healthcare entities and third parties to establish how e-PHI is shared and used. An SLA also establishes expectations of service provided.

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 communicate 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 having 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 someone 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: ____

   ____

   ____

Index