

HIPAA Certification: Administrator Third Edition

Instructor's Edition

PREVIEW

NOT FOR PRINTING OR INSTRUCTIONAL USE

HIPAA Certification: Administrator Third Edition

Series Product Managers: Caryl Bahner-Guhin and Adam A. Wilcox
Writer: Uday O. Ali Pabrai
Developmental Editor: Linda K. Long
Project Editor: Josh Pincus
Series Designer: Adam A. Wilcox

COPYRIGHT © 2009 Axzo Press

ALL RIGHTS RESERVED. No part of this work may be reproduced, transcribed, or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution, or information storage and retrieval systems—without the prior written permission of the publisher.

For more information, go to www.axzopress.com.

Trademarks

ILT Series is a trademark of Axzo Press.

Some of the product names and company names used in this book have been used for identification purposes only and may be trademarks or registered trademarks of their respective manufacturers and sellers.

Disclaimer

We reserve the right to revise this publication and make changes from time to time in its content without notice.

ISBN 10: 1-4188-6245-2

ISBN 13: 978-1-4188-6245-9

Printed in the United States of America

1 2 3 4 5 GL 06 05 04 03

NOT FOR PRINTING OR INSTRUCTIONAL USE

Contents

Introduction	iii
Topic A: About the manual.....	iv
Topic B: Setting student expectations	xxi
Topic C: Classroom setup.....	xxiv
Topic D: Support.....	xxvi
HIPAA basics	1-1
Topic A: HIPAA introduction.....	1-2
Topic B: Administrative Simplification	1-15
Topic C: HIPAA penalties.....	1-22
Topic D: HIPAA-related organizations	1-26
Topic E: HIPAA terminology.....	1-30
Unit summary: HIPAA basics.....	1-40
HIPAA Privacy Rule	2-1
Topic A: Introduction to privacy	2-2
Topic B: Terminology	2-13
Topic C: Notice of Privacy Practices.....	2-30
Topic D: Authorization	2-34
Topic E: Key parties impacted	2-39
Topic F: Minimum necessary.....	2-56
Topic G: Oral communications.....	2-66
Topic H: Health-related marketing	2-70
Topic I: Research.....	2-75
Unit summary: HIPAA Privacy Rule.....	2-81
Case study: Templates & getting started	3-1
Topic A: Planning for Privacy Rule compliance	3-2
Topic B: Administrative requirements	3-4
Topic C: Key privacy policy documents	3-10
Topic D: Flow of PHI	3-26
Topic E: Assessment and gap analysis	3-34
Topic F: Business associates	3-38
Topic G: Physician’s/dentist’s office scenario.....	3-45
Unit summary: Case study: Templates & getting started.....	3-52
Additional information and resources	A-1
Topic A: HIPAA Frequently Asked Questions (FAQs)	A-2
Topic B: HIPAA Security Rule FAQs.....	A-6
Topic C: Case study: P3P—A Privacy Standard	A-8
Topic D: Additional resources	A-10
Topic E: HHS Fact Sheet, Modifications to Final Privacy Rule	A-11
Topic F: HIPAA Academy and certification.....	A-15
Course summary	S-1
Topic A: Course summary	S-2
Topic B: Continued learning after class	S-3

Glossary

G-1

Index

I-1

PREVIEW

HIPAA Certification: Administrator Third Edition

Introduction

After reading this introduction, you will know how to:

- A** Use ILT Series training manuals in general.
- B** Use prerequisites, a target student description, course objectives, and a skills inventory to properly set students' expectations for the course.
- C** Set up a classroom to teach this course.
- D** Get support for setting up and teaching this course.

Topic A: About the manual

ILT Series philosophy

Our goal is to make you, the instructor, as successful as possible. To that end, our training manuals facilitate students' learning by providing structured interaction with the software itself. While we provide text to help you explain difficult concepts, the hands-on activities are the focus of our courses. Leading the students through these activities will teach the skills and concepts effectively.

We believe strongly in the instructor-led classroom. For many students, having a thinking, feeling instructor in front of them will always be the most comfortable way to learn. Because the students' focus should be on you, our manuals are designed and written to facilitate your interaction with the students, and not to call attention to manuals themselves.

We believe in the basic approach of setting expectations, then teaching, and providing summary and review afterwards. For this reason, lessons begin with objectives and end with summaries. We also provide overall course objectives and a course summary to provide both an introduction to and closure on the entire course.

Our goal is your success. We encourage your feedback in helping us to continually improve our manuals to meet your needs.

Manual components

The manuals contain these major components:

- Table of contents
- Introduction
- Units
- Appendix
- Course summary
- Glossary
- Index

Each element is described below.

Table of contents

The table of contents acts as a learning roadmap for you and the students.

Introduction

The introduction contains information about our training philosophy and our manual components, features, and conventions. It contains target student, prerequisite, objective, and setup information for the specific course. Finally, the introduction contains support information.

Units

Units are the largest structural component of the actual course content. A unit begins with a title page that lists objectives for each major subdivision, or topic, within the unit. Within each topic, conceptual and explanatory information alternates with hands-on activities. Units conclude with a summary comprising one paragraph for each topic, and an independent practice activity that gives students an opportunity to practice the skills they've learned.

The conceptual information takes the form of text paragraphs, exhibits, lists, and tables. The activities are structured in two columns, one telling students what to do, the other providing explanations, descriptions, and graphics. Throughout a unit, instructor notes are found in the left margin.

Appendix

An appendix is similar to a unit in that it contains objectives and conceptual explanations. However, an appendix does not include hands-on activities, a summary, or an independent practice activity.

Course summary

This section provides a text summary of the entire course. It is useful for providing closure at the end of the course. The course summary also indicates the next course in this series, if there is one, and lists additional resources students might find useful as they continue to learn about HIPAA.

Glossary





The glossary provides definitions for all of the key terms used in this course.

Index

The index at the end of this manual makes it easy for you and your students to find information about a particular concept.

Manual conventions

We've tried to keep the number of elements and the types of formatting to a minimum in the manuals. We think this aids in clarity and makes the manuals more classically elegant looking. But there are some conventions and icons you should know about.

<i>Instructor note/icon</i>	Convention	Description
	<i>Italic text</i>	In conceptual text, indicates a new term or feature.
	Bold text	In unit summaries, indicates a key term or concept. In an independent practice activity, indicates an explicit item that you select, choose, or type.
<i>Instructor notes.</i>		In the left margin, provide tips, hints, and warnings for the instructor.
	Select bold item	In the left column of hands-on activities, bold sans-serif text indicates an explicit item that you select, choose, or type.
	Keycaps like 	Indicate a key on the keyboard you must press.
 <i>Warnings prepare instructors for potential classroom management problems.</i>		Next to an instructor note, indicates a warning for the instructor.
 <i>Tips give extra information the instructor can share with students.</i>		Next to an instructor note, indicates a tip the instructor can share with students.
 <i>Setup instructor notes give a context for instructors to share with students.</i>		Next to an instructor note, indicates a setup the instructor can use before delivering a step or activity.

Activities

The activities are the most important parts of our manuals. Some are in a single-column format, presenting scenario-based, multiple-choice, or short-answer questions, as well as other types of activities. Activities use a two-column format when appropriate, such as for matching questions, or when there is a need for explanation, graphics, or clarifications. To the left, instructor notes provide tips, warnings, setups, and other information for the instructor only. Here's a sample:

Do it!

A-1: Planning for improvements

Exercises

1 Sequence the steps management should complete to plan for improvements.	
Select team members	<i>Identify potential processes</i>
Ask department heads for team members	<i>Select processes for improvement</i>
Select processes for improvement	<i>Establish objectives</i>
Communicate to employees	<i>Communicate to employees</i>
Identify potential processes	
Establish objectives	

PowerPoint presentations

Each unit in this course has an accompanying PowerPoint presentation. These slide shows are designed to support your classroom instruction while providing students with a visual focus. Each one begins with a list of unit objectives and ends with a unit summary slide. We strongly recommend that you run these presentations from the instructor's station as you teach this course. A copy of PowerPoint Viewer is included, so it is not necessary to have PowerPoint installed on your computer.

Course coverage

This course contains coverage of the Health Insurance Portability and Accountability Act (HIPAA) from the perspective of end users, such as nurses and administrators, responsible for delivering and supporting health-care related services. This course contains complete coverage of the Privacy Rule and information about resources available for obtaining information and the regulatory process.

This manual is useful as both a study guide and as a HIPAA Administrative Simplification reference. It is packed with hundreds of practice questions, technical sidebars, scenarios and templates that enable an understanding of specific HIPAA legislative compliance requirements. In addition, it contains many HIPAA project management templates for launching compliance-related enterprise initiatives.

Disclaimer

While students will learn about what is necessary for HIPAA compliance, they (or their organization) are responsible for bringing their organization into compliance. It is **strongly** suggested that organizations consult with legal and other professionals as they develop their compliance solutions.

About HIPAA Academy

The HIPAA Academy is about developing and validating HIPAA knowledge. The training program is designed to deliver the skills required for Certified HIPAA Professionals, Security Specialists and Administrators to be effective members of enterprise HIPAA implementation initiatives.

It is strongly recommended that members of the HIPAA implementation team have acquired the necessary skills to enable solutions required for meeting compliance requirements.

HIPAA Academy delivers solutions to assist organizations with their HIPAA initiatives in the areas of HIPAA Professional Services, HIPAA Assessment, Interim HIPAA Compliance Officer, HIPAA Project Managers and HIPAA Training and Certification.

For more details about HIPAA Academy and additional resources such as HIPAA FAQs and white papers access:

www.HIPAAAcademy.Net

Certification exams

The Certified HIPAA Administrator (CHA) exam validates knowledge and skills of end users that are responsible for delivery and support of health care services and administration.

The Certified HIPAA Professional (CHP) exam validates knowledge and skills in the core areas of HIPAA Administrative Simplification legislation, Transactions and Code Sets Requirements, Privacy Requirements and Security Requirements.

The Certified HIPAA Security Specialist (CHSS) exam validates knowledge and skill sets in:

- 1 The core domain areas of the HIPAA Security Rule: Administrative Safeguards, Physical Safeguards and Technical Safeguards. (75% of exam)
- 2 Security technology fundamentals including firewall systems, Intrusion Detection Systems (IDS), authentication solutions, IPSec, VPN, digital signatures, digital certificates, PKI, PGP, and International standards such as the ISO 17799. (25% of exam)

Exam grid

Exam name	Number	# of questions	Time	Passing score	Format
HIPADM-1	HIO-101	40	60 min.	75%	Standard
HIPPROF-1	HIO-201	60	60 min.	75%	Standard
HIPSEC-1	HIO-301	60	60 min.	75%	Standard

Exam fees

The Certified HIPAA Administrator exam fee is \$40. The Certified HIPAA Professional exam fee is \$150. The Certified HIPAA Security Specialist exam fee is \$195. Exam fees are not included in training costs. Exam fees are subject to change. All exams are delivered by Authorized Prometric Testing Centers.

Contact HIPAA Academy at www.HIPAAAcademy.Net for a complete list of Certified HIPAA Academy Training Partners and their course schedule.

Bring HIPAA Academy training, certification and executive briefs to your site. HIPAA Academy will customize the session to meet your specific requirements and time frames. Ask HIPAA Academy for flat rate pricing for an on-site customized session.

National accreditations and CE credits

State of Nebraska – Board of Public Accountancy

The Nebraska Board of Public accountancy is responsible for licensing and regulating Certified Public Accountants (CPA) and Public Accountants (PA) in Nebraska. Its mission is to protect the welfare of the citizens of the state by assuring the competency of licensed accountants and to serve the needs of the public accountancy membership by assisting them in complying with Nebraska law and Board-promulgated rules and regulations.

- Certified HIPAA Administrator (CHA): 8 CE credits
- Certified HIPAA Professional (CHP): 18 CE credits

West Virginia Insurance Commission

The West Virginia Insurance commission is charged with regulating all insurance companies licensed in West Virginia; that currently includes over 1,500 companies. The commission is responsible for licensing all West Virginia insurance agents. Its responsibility is to regulate the market in a fair manner to protect the insurance buying public and insure solvency of the companies.

- HIPAA Executive Brief: 2 CE credits
- Certified HIPAA Administrator (CHA): 8 CE credits
- Certified HIPAA Professional (CHP): 12 CE credits

The American Health Information Management Association (AHIMA)

The American Health Information Management Association (AHIMA) is the dynamic professional association that represents more than 45,000 specially educated health information management professionals who work throughout the healthcare industry. Health information management professionals serve the healthcare industry and the public by managing, analyzing, and utilizing data vital for patient care – and making it accessible to healthcare providers when it is needed most.

- HIPAA Executive Brief: 2 CE credits
- Certified HIPAA Administrator (CHA): 8 CE credits
- Certified HIPAA Professional (CHP): 18 CE credits

American Academy of Professional Coders (AAPC)

AAPC (American Academy of Professional Coders) membership spans all 50 states and several foreign countries as well. It is supported by a National Advisory Board made up of certified members representing clinics, facilities, payers and consulting firms. The AAPC National Advisory Board offers direct input into the certification programs, educational curricula, and membership services offered by the Academy. AAPC is also supported by a National Physician Advisory Board with physicians from many different specialties. The AAPC grants prior approval for continuing education programs based on the relevance of the program content to the medical coding and reimbursement profession.

- Certified HIPAA Professional: 18 CE Units

The American College of Healthcare Executives (ACHE)

The American College of Healthcare Executives is an international professional society of nearly 30,000 healthcare executives who lead our nation's hospitals, healthcare systems, and other healthcare organizations. ACHE is known for its prestigious credentialing and educational programs and its annual Congress on Healthcare Management, which draws more than 4,000 participants each year. ACHE is also known for its journal, the Journal of Healthcare Management, and magazine, Healthcare Executive, as well as groundbreaking research and career development and public policy programs. ACHE's publishing division, Health Administration Press, is one of the largest publishers of books and journals on all aspects of health services management in addition to textbooks for use in college and university courses. Through its efforts, ACHE works toward its goal of improving the health status of society by advancing healthcare leadership and management excellence.

- HIPAA Executive Brief: 2 CE credits
- Certified HIPAA Administrator (CHA): 8 CE credits
- Certified HIPAA Professional (CHP): 18 CE credits
- Certified HIPAA Security Specialist (CHSS): 16 CE credits

American Nurses Credentialing Center (ANCC)

The American Nurses Association established the ANA Certification Program in 1973 to provide tangible recognition of professional achievement in a defined functional or clinical area of nursing. The American Nurses Credentialing Center (ANCC) became its own corporation, a subsidiary of ANA in 1991. More than 150,000 nurses throughout the U.S. and its territories in 40 specialty and advanced practice areas of nursing carry ANCC certification. While the role for nurses continues to evolve, ANCC has responded positively by the re-conceptualization of certification and "Open Door 2000," a program that enables all qualified registered nurses, regardless of their educational preparation to become certified in any of five specialty areas: Gerontology, Medical-Surgical, Pediatrics, Perinatal and Psychiatric and Mental Health Nursing.

Because nearly every state nursing board in the country is accredited by the ANCC, nurses nationwide are able to use the Certified HIPAA Administrator (CHA) program to fill their own continuing education requirements.

- Certified HIPAA Administrator (CHA): 8 CE credits

About the author

Uday O. **Ali** Pabrai is a highly sought after HIPAA consultant and speaker. **Ali** has delivered keynote and other sessions at numerous conferences worldwide including National Council for Prescription Drug Programs (NCPDP), COMDEX, COMNET, Internet World and DCI's Internet Expo. **Ali** is an accomplished expert in the areas of HIPAA, e-business, enterprise security policy and architecture.

Ali has delivered HIPAA Executive Briefs and the Certified HIPAA Professional (CHP) program nationally. His attendees have included hospitals, pharmacies, legal professionals, physicians, office administrators, clinicians, HIPAA compliance officers as well as IT professionals such as CISSPs, transactions and security experts. **Ali**'s clients have included Blue Cross Blue Shield affiliates, Wells Fargo, Seabury and Smith/Marsh and many others.

Ali created the industry leading CIW program and is the co-creator of the highly successful Security Certified Program (SecurityCertified.Net). **Ali** is the author of numerous books and articles on HIPAA, privacy, e-business, security and business threats. At ecfirst.com, **Ali** developed HIPAAShield, a HIPAA security-related implementation methodology.

Pabrai invited by the National Council for Prescription Drug Programs (NCPDP) to discuss "HIPAA Privacy and Security"

In the health care arena, pharmacy leads the way among electronic health care claims. Over 88 percent of the pharmacy claims in 1999 were submitted electronically, according to Faulkner & Gray's 2000 Health Data Dictionary. It is through the diligent work of NCPDP members that our standards keep up with the ever-evolving marketplace. NCPDP is also known for its annual conference and other meetings. Since NCPDP is an ANSI-accredited Standards Development Organization, the attendees at NCPDP's meetings are leading the industry in both the business and technical arenas. No other organization brings together the diversity of industry leaders and decision-makers that NCPDP does.

With cutting-edge educational conferences and technical work groups, NCPDP offers you an unmatched opportunity to learn what drives some of the hottest issues in health care. NCPDP members are responsible for developing many of today's key innovations in pharmacy and health care.

NCPDP's Educational Forums are designed to educate industry colleagues on important issues relating to the pharmacy services sector of the health care industry. These sessions are open to all interested parties, for a fee. On Tuesday, August 27, 2002 at the Renaissance Washington DC Hotel, NCPDP held an Educational Forum on HIPAA Privacy and Confidentiality.

Uday O. **Ali** Pabrai was invited by the NCPDP for the conference in Washington, DC. **Ali** delivered a session on "HIPAA Privacy and Security: Administrative Requirements."

Notes from the author

I hope you are excited about HIPAA and take advantage of the legislation to transform skills and core business practices. It all starts with PHI, but will end with several e-business initiatives. At the HIPAA Academy, we are very passionate about the legislation and associated solutions. In the long term, the positive impacts of HIPAA will not be insignificant. We are excited. HIPAA will result in a transformation of your business for the better. HIPAA initiatives will lead to more transparency between the organization and patients. HIPAA is about transformation, transparency and the application of technology.

Whether you are as excited (or depressed), it will be an emotional experience. Do not hesitate to drop me a note about your experiences. I can be reached via e-mail at Pabrai@HIPAAAcademy.Net.

Acknowledgements

First, I would like to thank all the students of the HIPAA Academy. Their industry insight, review and experiences have had a terrific impact in furthering my understanding of the HIPAA regulations and development of practical solution alternatives.

Matt McCright – a good friend and a security expert, worked closely with me in reviewing and enhancing the content in several areas, especially security. Matt – thank you.

Gary Bard and Jasvinder Kakar – thank you for your disciplined approach in reviewing solutions in the transactions area, especially products such as Microsoft's BizTalk Accelerator and Sybase's HIPAA Studio. Mark Glowacki, Tom Eilers and Lorna L. Waggoner – thank you for reviewing and assisting to further improve the quality of the material.

Linda K. Long – I am grateful for your thorough professionalism in editing the work. It was fun working with you on this initiative.

Allen Nguyen, my partner and good friend. There is an incredible strength in peace, patience and perseverance. I have always placed trust and faith in our relationship.

This work has involved terrific and relentless coordination efforts from Michael T. Curry. Mike – thanks. Love your attitude and humor. Allen, Mike and I are very appreciative of the efforts of several individuals including Bhavan Mehta, Jerome Schuster, Lisa Barton, Tad Anhalt, Hemant Birari, Sunny Chng, Suhas Sankolli and Amita Mehta. Sunny – I have to say that you have delivered an exceptional Web site in building HIPAAAcademy.Net – awesome work! I am especially grateful to Scott Phillips for assisting me immensely with several HIPAA projects.

To all my friends at Prometric, NCPDP, NetG, MeasureUp/Dice, CESC and Course Technology – thank you. This has been a genuine team effort between several Thomson Learning enterprises.

To organizations that were a part of my roots and learning – Maneckji Cooper in Mumbai, Air Force Central School in New Delhi, and the Indian High School in Dubai, UAE – thank you, I am grateful. To organizations that extended my thinking forever – Clemson University, Illinois Institute of Technology, Wells Fargo, Fermi National Accelerator Laboratory, and the U.S. Department of Energy – I am sincerely appreciative.

Tashi and Nathan – no need to “control your excitement!” Have fun and thank you for your passionate support. Mummy, Ammee, Baba, Ashkan and most of all Ammajaan – thank you for your prayers and faith. Papa, I love you and miss you!

Nazeela – your prayers, patience and unquestioned support cannot be appreciated enough. You have an amazing peace about yourself. I am truly blessed to have you as my companion for life. Most of all, thank you – aapka ali.

And finally, to all my readers, as you get started, a word of caution: Control Your Excitement!!!!

Dedication

To Jaanu, my wife and dearest friend, Nazeela. I have found my peace and thank God for bringing us together to share and care. To our future – **Arshiyaa and Ariyamaan.**

Uday O. Ali Pabrai

Testimonials

“Excellent delivery, well paced. The strength of the course was entirely the knowledge and presence of the instructor. Ali was knowledgeable and entertaining. Course rating 10. Instructor rating 10.”

Elisa Chase, State of Connecticut

“Instructor was lively, personable. Course was very good, informative.”

Astread Ferm-Poole, Department of Social Services, State of Connecticut

“Outstanding course. Excellent overview. Course rating 10. Instructor rating 10.”

Mass Mutual Financial Group

“The strength of the course was the enthusiasm and knowledge of the instructor.”

Bob Mallick, Mass Mutual Financial Group

“Allan did an excellent job in instructing us on HIPAA compliance. I enjoyed his class and it was very beneficial to me. I like the small class size we were in- it made it easy to discuss topics and issues we had. The most important thing was the ability to ask questions or discuss issues that we had at any point during the seminar and not having to wait till the end for a question and answers session.”

Julie Bain, J.D. Bonner, MD

“I was very apprehensive about HIPAA going into this course. To be honest, I was very ignorant of HIPAA. However, by the end of the day, I realized in many areas our office was already HIPAA compliant. But I learned many things we needed to incorporate into our clinic in order to meet compliance. This one-day course was very informative and helpful for me.”

Jonesboro Surgery Clinic

“I feel better about HIPAA in many ways, but realize I have a lot of work still to do!”

HIPAA Administrator Student

“The course was excellent for learning the basics of HIPAA. The material was easy to understand considering the difficult and complicated subject.”

Kathy Atchley, St. Bernard’s Medical Center

“Very good instructor. The material was well presented and is easy to understand for such a difficult subject.”

HIPAA Administrator Student

“Chuck was an excellent instructor. He gave a lot of examples and truly understood the material.”

HIPAA Professional Student

“Chuck made class enjoyable while teaching professionally. Great job!”

HIPAA Professional Student

“I enjoyed the course very much. Chuck was very knowledgeable in the HIPAA regulations and effectively communicated them.”

HIPAA Professional Student

“Excellent class! The instructor was fantastic!”

HIPAA Professional Student

“Excellent course. The most informative I have ever attended.”

Lynn Simmons, Jonesboro Surgical Assoc.

“Allan is a very good instructor. He made HIPAA fun to learn.”

HIPAA Professional Student

“The class was very good. The instructor was very knowledgeable. He spent a lot of time making sure we understood the material and how to use it. When you finish this class you should be able to pass the certification test.”

Kathryn French

“An excellent intensive program with practical helpful information that can be used in the work setting. Very practical.”

Phyllis Woolverton, St. Bernard’s Medical Center

“An excellent intensive course with helpful information that can be used in everyday practice.”

HIPAA Professional Student

“Allan does an excellent job of breaking HIPAA down into understandable “English” instead of lawyer language.”

HIPAA Professional Student

“Allan is a great instructor who effectively uses examples to explain issues, makes the course enjoyable and encourages discussions.”

HIPAA Professional Student

“Great overview!”

Robert Savage, USDC

“The instructor was extremely knowledgeable about this subject and willing to answer all questions. She was also able to put the information in Layman’s terms.”

Andi Cady, Hollywood Pediatrics

“A tremendous amount of material explained in a coherent manner.”

Jason Schulman, Hollywood Pediatrics

“The Executive Brief was a very helpful overview. I really didn’t understand the scope of HIPAA legislation before this presentation. Thanks!”

Deborah Jones, DPM

“I didn’t expect to get as much information as I did in the 2 hour time frame. This was a worthwhile presentation... The instructor was extremely prepared and the course was excellent!”

A student in the Ft. Lauderdale Executive Brief

“The Executive Brief was very informative.”

Phil Salon, Lansing Fire Department

“The 2-hour class was very helpful in giving an overview and clarifying several areas.”

Jim Fisher, Correctional Medical Services

“The Executive Brief was informative.”

Deb Atherton, Alliance-HNI

“The Executive Brief was very informative. I am looking forward to the next step in the process.”

Roby Purtec, Alliance-HNI

“I attended the “Executive Brief” 2 hour session. It was definitely useful, was well organized, and would recommend to others.”

Ken Ammerman, Archy’s & Sons Inc.

“The Executive Brief was highly informative with specific scenarios. These will be helpful in formulating policies and procedures.”

Candy Watters, Messa

“The Certified HIPAA Administrator is a good course. I found out a lot of great information in a short period of time. Very worthwhile.”

Tom Edgeton, MediNotes

“Everyone needs the Administrator course!”

Cathy Halston, MediNotes

“I now have a much better understanding of HIPAA privacy and terms. I will have more confidence in speaking about HIPAA with my clients after taking the Administrator class.”

A MediNotes account executive

“I was very nervous to break into small groups to write a compliancy plan. Listening to other groups present their plans was very useful to me. Everyone thinks of different things, everyone has new, different ideas. Thanks for making me do that!”

Chris Boyken, Duncan Heights, Inc./Iowa Association of Homes and Services for the Aging

“As a project manager for DHS Oklahoma, I found the training session held by Ali a very informative and productive use of my time. The session covered the key aspects of HIPAA and how it affects government and healthcare organizations along with the key high-level tasks that need to be completed to be HIPAA compliant. Ali also shared his insights and experiences with the group and this was extremely beneficial to me. I would recommend that anybody that needs a decent overview of HIPAA must attend this session. It will help you get out of the starting block in a hurry.”

Sarjoo Shah, HIPAA Project Manager

Department of Health Services (DHS), State of Oklahoma

“The instructor was very knowledgeable about HIPAA Compliance. This is the most information I’ve gotten about HIPAA. I’ve been to other HIPAA training and I have never gotten the wealth of information I received today.”

Inez Wondeh, Peninsula Medical Group

“The class was very well paced with information in all areas of the new requirements.”

Kellien Duncan, County of Alameda, State of California

“A fast pace, informative overview of the Administrative Simplification portion of the HIPAA legislation. Excellent reference tools and indicators to help administrators identify the ‘next course of action’.”

Deborah Windish, Michigan Academy of Family Physicians (MAFP)

“This is a good overview. Most of us that are involved with HIPAA often feel overwhelmed. I’m still overwhelmed but I can finally see the light at the end of the tunnel.”

Deeann M. Biondi, SET SEG, Inc.

“Excellent course to provide an overview of HIPAA in a short period of time. Excellent and very knowledgeable instructor who was able to cover key issues of HIPAA in an easy to understand manner and in a very short time (2 hours).”

Steve Trosty, AP Assurance

“Ali’s presentation was both highly informative and a basic building block for implementation of HIPAA regulations. This was a fundamental step toward a large training opportunity for New Horizons of Michigan.”

Mark McManus, Sr., Chairman, New Horizons of Michigan

“Excellent overview of HIPAA regulations. I look forward to attending the advanced programs on the implementation.”

Steven Shurts, Harris HeathTrends, Inc.

“Was very helpful, I would even call it vital. I will urge all my co-workers and associates to get trained. Everyone should attend the 3-Day Professional boot camp. I wish I’d done this last year.”

Trish Chandler, Sharp, Inc.

“We covered an enormous amount of material in a short period of time. The Certified HIPAA Instructor made complex and hard to understand material easy to learn!”

Joe Flippin

“The Certified HIPAA Professional course has not only enlarged my knowledge and expertise, but also opened wider the door to professional and entrepreneurial opportunities.”

Laurice Green, Child and Family

“I enjoyed the class. I initially thought that healthcare portion would be hard to follow coming from a technical background. The course and the regulations related a lot to network technologies. I just passed the CISSP exam and combined with this credential, I feel this will help my consulting business tremendously.”

Lisa Jones, Slipknot Technologies

“I have an EDI X12 background in distributing manufacturing and finance. I am familiar with mapping software and principles. This course explained many new terms and procedures in an easy to learn style and I would recommend it to people with or without a healthcare background.”

Ernie Schum, Schum Consulting, Inc.

“The course by itself is outstanding! But Mark took it to the next level.”

Moqueet Syed, Batuta, Inc.

“Well organized information. A solid understanding of the topic was presented as well as insights into opportunities that will be available as a result of this initiative.”

Terry Roberts, Business Systems Engineering

“I realize the professional importance of understanding this information. I really believe my professional life is dependent on acquiring this knowledge. It is a lot of information in a short time, but I have a reference book. I am accustomed to Federal and State rules and regulations and this is just one more very important tool to do a better job. I have now been given the tools and opportunity to succeed. I will recommend this course to others without hesitation.”

John Palmer, Shelby County Government, Oakville Healthcare Center

“The information in the course is clear and concise and will serve as a good HIPAA reference!”

Gina Winchester, Sharp, Inc.

“The class was extremely informative. I’ve learned many new things and also received confirmation that I understand certain aspects of HIPAA correctly.”

Darcey Gartner, Vista Healthplan, Inc.

“I have learned a tremendous amount!”

Victoria Sunshine

“I’m amazed at how much I was able to learn in just 3 days. I feel very confident that the information I picked up, the practical exercises, and the class interactions provided me with what I need to help my customers through the HIPAA hoop! The instructors were knowledgeable and always willing to address specific questions. All in all, this was a great experience that will benefit me, my clients, and my company!”

Cathy Pitt, Hewlett Packard

“This was by far the most in-depth HIPAA course I have attended. The instruction staff is very knowledgeable of the Administrative Simplification Title. They did a great job of operating a comfortable environment.”

Kelly Gruber, Des Moines Orthopedic Surgeons

“I have been following HIPAA progression for 2 years and found this course the most comprehensive of all my studies, especially in the privacy section. The instructor seemed to take personal responsibility to assure the students understood that this section was important to all areas of the HIPAA legislation... Lorna is an excellent instructor, her examples of in-the-box and out-of-the-box were excellent.”

Betty Aukee, ADP

“The task of bringing my client to HIPAA compliance was dumped in my lap. As a consultant more on the management side of the healthcare industry, I felt overwhelmed when given the responsibility. Being only slightly familiar with the medical transactions, codes and procedure, I thought it impossible to even grasp HIPAA from a class. Boy was I wrong! I now am aware and feel competent in my knowledge of the scope of HIPAA, and I am convinced that it will be evident in my report/briefs to my clients. Thank you HIPAA Academy!”

Anita Herron, Primary Care Partners

“This class was very intense and extremely beneficial at breaking down the core components of Title II. I was already familiar with HIPAA and had attended previous courses, however I feel this class brought it all together for me.”

Tracie Martin, Baylor Health Care Systems

“I am excited to learn about the HIPAA Academy and its services.”

Bill Bendall, SeniorCare, Inc.

“I would recommend this course to anyone in the medical field responsible for HIPAA Compliance. I had very little knowledge of HIPAA and the medical industry as a whole. This course educated me in these areas. I feel that I came away with a good base to build on. I believe that many people will struggle with compliance without this help!”

Tom Agnitsch, ANE Technology Services

“One of the strengths of the course was the overview of upcoming changes to HIPAA legislation.”

Karla Combs, Lipscomb & Pitts

“What an eye opener. Before the course I had only a vague idea of the implications and scope of HIPAA. Now I realize how much work is left to be done to get into compliance and how this is going to touch every aspect of the health care industry.”

James Cerney, J.C. Solutions

“I would highly recommend the HIPAA Academy to anyone in healthcare that wants to obtain the knowledge that will be crucial to implement HIPAA legislation in their organization. I found the instructors and the course material to be first rate and the information taught will help healthcare professionals at all levels to navigate the risky waters of HIPAA.”

Joel H. Snook, CPA, Chief Financial Officer, St. Petersburg, FL

“The Certified HIPAA Professional course is one of the best, if not the best, courses on the down and dirty of HIPAA. I highly recommend this course as a “Train the Trainer” for health care organizations looking to comply with current and pending requirements. This course is going to help me immensely in architecting solutions for organizations to comply with Title 2 requirements.”

Bob Tahmaseb, CISSP, Systems Engineer, RSA Security Inc.

“The Size and scope of the HIPAA legislation was brought into perspective buy the HIPAA Academy. I now have a far greater understanding of the impact on the entire healthcare industry. The importance of the Professional class can not be under stated.”

Allan Gilbreath, Network Edge

“The strength of the course was the instructor’s knowledge base beyond the scope of requirements for certification. This was a great learning experience and a non-intimidating atmosphere.”

Francoise Ager, AT&T

“Fast paced, well organized, data packed, lively and entertaining.”

Sumner Buck, VP, Open Road Technologies

“The HIPAA Academy training course is comprehensive and practical. I walked away from this course with a very clear understanding of the Administrative Simplification components of HIPAA. This course allowed me to get my arms around some very complicated requirements and helped me piece the requirements together. I was surprised at how helpful it was because I had a fairly comprehensive understanding to HIPAA prior to taking the course. I highly recommend it to anyone who will be involved with HIPAA compliance, in fact, anyone who is involved with HIPAA would be foolish for not taking this course.”

Teri Ann Lawyer, HIPAA Attorney, Pingel & Templer, P.C.

“The Certified HIPAA Professional course is a great source of information. It really lets you get your hands around what HIPAA and the Administrative Simplification Title mean and how it will change business. Not only does the course show business requirements, but the business opportunities that will arise as well.”

Chris Reynolds, ExecuTrain of Nebraska

“They are the only organization that could help me achieve my goal of certification. I would rate them very highly. They have a broad background of HIPAA knowledge.”

Tom Eilers, HIPAA Consultant & Project Manager

“This is by far the most comprehensive course I have ever taken. The instructors’ personality and knowledge of the course really moves things along with out making you feel too overwhelmed. For anyone involved with HIPAA in any capacity, I wholeheartedly recommend attending this course.”

Barbara Slocumb, Orlando, FL

“The Certified Professional Course is a great course packed with useful information.”

Margie Pullock, Orlando, FL

“The instructor was great, his enthusiasm for the course material was only surpassed by his knowledge of the material.”

Lori Lederman, Orlando, FL

“This class gave me an overview of the steps needed to become HIPAA Compliant. The most impressive aspect of the course is the amount of information covered in such a short period of time. I had no idea how many areas needed this much attention. This has really given me the foundation to cover all the bases.”

Lorna Waggoner, Owner, Sales for Hire

Topic B: Setting student expectations

Properly setting students' expectations is essential to your success. This topic will help you do that by providing:

- A description of the target student at whom the course is aimed
- A list of the objectives for the course
- A skills assessment for the course

Course prerequisites

There are no specific prerequisites for this course.

Target student

This course will help students better understand HIPAA's Administrative Simplification Act. They will learn how to create a framework for initiating and working towards a blueprint for HIPAA compliance. Candidates for this course will come from the health care, Information Technology (IT), and legal industries.

Course objectives

You should share these overall course objectives with your students at the beginning of the day. This will give the students an idea about what to expect, and will also help you identify students who might be misplaced. Students are considered misplaced when they lack the prerequisite knowledge or when they already know most of the subject matter to be covered.

After completing this course, students will know how to:

- Understand the purpose of HIPAA legislation; interpret HIPAA's Administrative Simplification title; identify penalties for noncompliance; identify organizations associated with HIPAA; and understand HIPAA-related terminology and definitions.
- Interpret the core requirements of the Privacy Rule; explain the purpose and key sections of Notices and Authorizations; identify key parties impacted by the Privacy Rule; explain Privacy Rule requirements for oral communications and marketing; and describe conditions for PHI use or disclosure for research purposes.
- Describe the Privacy Rule's administrative requirements; examine the flow of PHI within and outside an organization; identify the steps involved in site assessment and gap analysis; analyze the requirements for business associates; identify the key elements of a Business Associate Contract; and examine Privacy Rule compliance scenarios.

Skills inventory

Use the following form to gauge students' skill level entering the class (students have copies in the introductions of their student manuals). For each skill listed, have students rate their familiarity from 1 to 5, with five being the most familiar. Emphasize that this is not a test. Rather, it is intended to provide students with an idea of where they're starting from at the beginning of class. If a student is wholly unfamiliar with all the skills, he or she might not be ready for the class. A student who seems to understand all of the skills, on the other hand, might need to move on to the next course in the series.

Skill	1	2	3	4	5
Describe the motivation and drivers for HIPAA legislation					
Describe the components of HIPAA's Administrative Simplification title					
Identify penalties for noncompliance					
Identify organizations associated with the HIPAA legislation					
Describe HIPAA-related terminology and definitions					
Interpret the core requirements of the Privacy Rule					
Identify key Privacy Rule terms and definitions					
Explain the purpose and key sections of Notice and Consent documents					
Identify the need for Authorizations					
Identify key parties impacted by the Privacy Rule, including patients, parents, and government agencies					
Describe minimum requirements					
Explain the Privacy Rule's requirements for oral communications					
Define health-related marketing and communications requirements					
Describe conditions for PHI use or disclosure for research purposes					
Examine next steps for compliance with the HIPAA Privacy Rule					
Describe the Privacy Rule's administrative requirements					

Skill	1	2	3	4	5
Identify key elements of Notice and Authorization documents					
Examine the flow of PHI within and outside an organization					
Identify the steps involved in conducting an assessment analysis					
Identify the steps involved in conducting a gap analysis					
Analyze the requirements for business associates and step through the model Business Associates Contract published by the Office for Civil Rights (OCR)					
Step through a Privacy Rule compliance scenario for a small physician's or a dentist's office					

Topic C: Classroom setup

In addition to a manual, each student should be provided with a writing pad and pens or pencils for jotting down notes and questions. Students should have a comfortable place to sit and ample table space to spread out their materials.

This course does not require each student to have access to a personal computer during class. However, we have provided some Word documents for use in selected activities. You should print these documents and distribute them to the class. If students want to edit the Word files after class, they will need a Windows-based PC with Microsoft Word 97 (or later) installed.

Computer requirements

If you wish to use the PowerPoint presentations, you'll need the following:

- A Pentium-class or better computer
- A keyboard and a mouse
- Windows 98, NT, 2000, or XP
- A minimum of 32 MB RAM, depending on your operating system
- CD-ROM drive
- A Super-VGA monitor
- An overhead monitor projector
- PowerPoint 2000 or later, or PowerPoint Viewer (included with the presentation files)

First-time setup instructions

If necessary, download the PowerPoint presentations for the course as follows. You can download the presentation files directly to the instructor machine, to a central location on your own network, or to a disk.

- 1 Connect to www.axzopress.com.
- 2 Under Downloads, click Instructor-Led Training.
- 3 Browse the subject categories to locate your course.

Setup instructions for every class

Every time you teach this class, you'll need to do the following:

- 1 If necessary, download the Word documents (student data files) for the course as follows:
 - a Connect to www.axzopress.com.
 - b Under Downloads, click Instructor-Led Training.
 - c Browse the subject categories to locate your course. Then click the course title to display a list of available downloads.
 - d Click the link(s) for downloading the Student Data files.

- 2 Print the Word documents and distribute them to every student. Document titles and file names are listed in the following table.

Document title	File name
Business Associate Contract	BAC.doc
Notice of Privacy Practices	Privacy_Practices.doc
Privacy Authorization Form — For Research Purposes Including Treatment	Research_Purposes_Treatment.doc
Privacy Authorization Form — Physician’s Office and Covered Entity	PhysicianOffice_CoveredEntity.doc
Privacy Authorization Form — Physician’s Office and Patient	PhysicianOffice_Patient.doc
Request for Access to Patient’s Health Information	Access_Health_Info.doc
Request for Amendment of Health Information	Amend_Health_Info.doc

Topic D: Support

Your success is our primary concern. If you need help setting up this class or teaching a particular unit, topic, or activity, please don't hesitate to get in touch with us.

Contacting us

Please contact us through our Web site, www.axzopress.com. You will need to provide the name of the course, and be as specific as possible about the kind of help you need.

Instructor's tools

Our Web site provides several instructor's tools for each course, including course outlines and answers to frequently asked questions. To download these files, go to www.axzopress.com. Then, under Downloads, click Instructor-Led Training and browse our subject categories.

Unit 1

HIPAA basics

Unit time: 120 minutes

Unit objectives:

- A** Understand motivation and drivers for HIPAA legislation.
- B** Examine HIPAA's Administrative Simplification title.
- C** Identify penalties for noncompliance.
- D** Identify key organizations associated with the HIPAA legislation.
- E** Describe HIPAA-related terminology and definitions.

Topic A: HIPAA introduction

Explanation

The health care industry is a trillion dollar industry that is undergoing a rapid transformation. There are about 10 million individuals employed in the health care industry and the Department of Labor recognizes 400 different job titles. The health care delivery industry is highly fragmented and very complex; however, it is beginning to change the way it electronically processes information.



The *Health Insurance Portability and Accountability Act* (HIPAA) is about insurance portability, fraud, and administrative simplification. This course examines the Administrative Simplification title of the HIPAA legislation. This title is watershed legislation for health care information systems. It will result in substantial investment in e-business initiatives and deployment of security technology in the health care and insurance industries.

The emphasis the HIPAA Administrative Simplification legislation places on *Protected Health Information* (PHI) cannot be overemphasized. The penalties detailed in the legislation for violations in this area further reinforce this point.

HIPAA compliance starts with PHI but ends invariably by impacting business processes, communications, and systems. The HIPAA standards (rules) are voluminous. The provisions within the legislation are moving targets, with a need to track requirements in the areas of transactions, code sets, identifiers, privacy, and security. The key is to get started and better understand the legislation to determine options and solutions to bring the organization into compliance. It is not a question of if your organization will be compliant with HIPAA, but when.

The sooner an organization gets started with HIPAA compliance initiatives; the better their chance of creating an enterprise infrastructure that will be much more efficient and effective in delivering medical services and protecting medical information. HIPAA makes business sense because it forces the issue of electronic transactions. It also forces the issue of protecting medical information that flows through the organization and outside. These and other factors, are leading almost all health care enterprises to put HIPAA initiatives as a priority.

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) became law on August 21, 1996. HIPAA is also known as:

- Public Law 104—191 [H.R. 3103]
- The Kennedy-Kassebaum bill

The U.S. Congress passed HIPAA to:

- Improve portability and continuity of health insurance coverage in the group and individual markets
- Combat waste, fraud, and abuse in health insurance and health care delivery
- Promote the use of medical savings accounts
- Improve access to long-term care services and coverage
- Simplify the administration of health insurance

HIPAA is not only about ensuring the continuation of health insurance for individuals changing employment, but it is about protecting the privacy of patient records and any other patient identifiable information in any media form.

In order to enable these sweeping goals the original HIPAA legislation included a number of titles, each addressing a different facet of the overall objective.

Title	Description
Title I	Health Care Insurance Access, Portability and Renewability
Title II	Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform
Title III	Tax-related Health Provisions
Title IV	Application and Enforcement of Group Health Insurance Requirements
Title V	Revenue Offsets

Title I

Title I of HIPAA ensures and enhances insurance access, portability, and renewability. Under this title, HIPAA provides the following new protections for millions of working Americans and their families:

- Increases the ability to get health coverage when starting a new job
- Reduces the probability of losing existing health care coverage
- Helps workers maintain continuous health coverage when changing jobs
- Helps workers purchase health insurance coverage on their own if they lose coverage under an employer's group health plan and have no other health coverage available.

Specific protections of this title include:

- Limits the use of pre-existing condition exclusions
- Prohibits group health plans from discriminating by denying you coverage or charging you extra for coverage based on your or your family member's past or present poor health
- Guarantees certain small employers, and certain individuals who lose job-related coverage, the right to purchase health insurance
- Guarantees, in most cases, that employers or individuals who purchase health insurance can renew the coverage regardless of any health conditions of individuals covered under the insurance policy

In short, Title I of the HIPAA legislation is intended to lower the probability of an individual or family losing existing coverage, to ease the ability to switch health plans, and to help those who are without coverage to find it on their own if they lose their employer's plan and have no other coverage available. Regulations in support of Title I have (arguably) been relatively well integrated into the American health care infrastructure today.

Title II

HIPAA Title II is about preventing health care fraud and abuse; administrative simplification; and protecting the privacy and confidentiality of patient records and any other patient identifiable information in any media form. This course covers the details of HIPAA Title II.

Titles III, IV, and V

In a similar manner, Congress and the various regulatory agencies that play a role in the American health care delivery and financing infrastructure have generally addressed the last three titles of HIPAA. These titles are: Tax-related Health Provisions, Application and Enforcement of Group Health Insurance Requirements, and Revenue Offsets.

Motivation for HIPAA

Today, health plans, hospitals, pharmacies, laboratories, doctors, and other health care entities use a wide array of systems to process and track health care bills and other information. Hospitals and doctor's offices treat patients with many different types of health insurance and must spend time and money ensuring that each claim contains the format, codes and other details required by each insurer. Similarly, health plans spend time and money to ensure their systems can handle transactions from various health care providers and clearinghouses. Congress has identified some portion of these transaction-related expenses as waste.

Congress included provisions in HIPAA to require the *Department of Health and Human Services* (HHS) to adopt national standards for certain electronic health care transactions, codes, identifiers, privacy, and security.

HIPAA also set a three-year deadline for Congress to enact comprehensive privacy legislation to protect medical records and other personal health information. When Congress did not enact such legislation by August 1999, HIPAA required HHS to issue health Privacy regulations. The HHS draft Privacy regulations were initially released in November 1999. The draft was an exercise in political maneuvering, exercising influence, and consensus building. HHS worked through more than 52,000 formal comments concerning the initial draft Privacy regulations. The final Privacy Rule was released August 14, 2002. In the final Privacy Rule, requirements for consent were loosened, while notice requirements were tightened. The final Security Rule was released on February 20, 2003, setting a compliance date of April 21, 2005 for all covered entities except small health plans—for them the compliance date is April 21, 2006.

Why is privacy part of HIPAA?

Security and privacy standards can promote higher quality care by assuring consumers that their personal health information will be protected from inappropriate uses and disclosures. A survey conducted by Princeton Survey Research Associates for the California Healthcare Association submits that Americans are increasingly concerned about the loss of privacy in every-day life, and especially about their health information.

In the last two decades, the lack of privacy has led people to withdraw from full participation in their own health care because they are afraid that their most sensitive health records will fall into the wrong hands, leading to discrimination, loss of benefits, stigma, and unwanted exposure.

The study found that one out of every six people engages in some form of privacy-protective behavior to shield themselves from the misuse of health information, including withholding information, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and—in the worst cases—avoiding care altogether.

This is especially true when researchers investigated groups of people that have cancer, AIDS, sexually transmitted diseases, substance abuse, or mental illness. These privacy-protective behaviors cost our nation billions of dollars in lost productivity and in increased costs for dealing with diseases that have progressed needlessly.

Addressing privacy and security issues via HIPAA regulations will cost the American health care industry (and its customers) somewhere between \$17 billion over the first decade and more than \$22 billion over the first five years, depending on which experts you believe. That seems like a lot of money. Why bother?

The intent is that uniform national standards will save billions of dollars each year for health care businesses by lowering the costs of developing and maintaining software and reducing the time and expense needed to handle health care transactions. HHS estimates that compliance will generate cost savings associated with implementing HIPAA's transaction standards of approximately \$29 billion over ten years.

If the transaction standards are implemented by providers and payers together, as intended by congress, consumers and health care organizations should benefit. Gartner Group researchers have suggested that many health care providers are depending on their vendors and clearinghouses for compliance. If this suggestion is accurate, then the health care industry will not reap savings to the extent intended in the legislation.

Health care organizations that focus their efforts on achieving full compliance in provider/payer transactions will be much better positioned than their peers waiting for vendor or clearinghouse solutions. Similarly, those organizations that give security and privacy compliance the appropriate priority will be able to more quickly refocus on their core competencies. Security compliance will be difficult, and health care organizations that wait might have a difficult time avoiding penalties.

The health care industry today is rapidly transforming the way it electronically processes information. One significant challenge in electronic information processing is coordinating the exchange of information throughout an enterprise, while also ensuring the security of the exchanged information.

In the health care industry, providers, insurers, and plans use many different electronic formats. This results in inefficient transactions when a patient's medical records and payment information needs to be moved between providers, insurers, and plans. Further, there are minimal procedures, policies, and technologies in place to secure the movement or storage of all such medical records and related payment information.

HIPAA is a defining standard for how the health care industry will handle patient medical records and related payment information in an efficient, private, and secure manner. This is similar to how all businesses have to secure information related to employees, customers, and suppliers.

In addition, HIPAA provisions will result in e-business initiatives that will substantially reduce the costs of processing medical claims and transactions. One of HIPAA's goals is to provide national standards for consistent data formats for health care transactions. Besides data format consistency, another key benefit from HIPAA compliance is the substantial reduction in paper-handling costs for health care claims. These costs are likely to be reduced significantly.

Health care applications that have been used to maintain, transform, transmit, verify, or audit transactions are being seriously impacted as a direct consequence of HIPAA.

There are other challenges that many organizations must face when making relatively radical changes in any of their core line-of-business systems. Many larger physician's practices/clinics, hospitals, and other more complex health care organizations depend upon an intricate web of internal, outsourced, and service-provider applications. Many of these applications use, display, or store protected health information. Some examples of these kinds of systems include (but are not limited to):

- Call/contact center systems
- Claims clearinghouses
- Customer relationship management systems
- Document imaging management systems
- Emergency department systems
- Enterprise resource planning systems
- General financial systems
- Materials management systems
- Nurse triage systems
- Operating room systems
- Patient accounting/billing systems
- Practice management systems
- Technology-enabled marketing systems

Many organizations also attempt to increase efficiencies by tightly coupling systems and implementing an automated workflow. In a Gartner Group research note, authors M. Davis, R. Dearborn, and T. Berg argue that a significant number of health related businesses are using HIPAA mandates to justify replacement of a number of key applications.¹ It is critical that you keep in mind that in an integrated infrastructure, characterized by an automated workflow and tightly-coupled systems, any significant change in any one system will also require that you test (possibly even modify) other systems. This kind of effort can be notoriously difficult and time consuming. That said, HIPAA compliance still requires that most health related organizations make these kinds of relatively high-risk changes.

HIPAA's impact

HIPAA will result in:

- Standardization of electronic, administrative, and financial health care transactions
- Unique health identifiers for employers, health plans, health care providers, and eventually individuals
- Security standards protecting the confidentiality and integrity of individually identifiable health information, past, present or future
- Privacy of protected health information
- Standards for electronic medical records

HIPAA impacts *covered entities* such as health plans, health care clearinghouses, and health care providers. These covered entities have to meet the requirements of HIPAA.

Covered entities will also need to work with business associates, agents, and contractors that have access to health information, for example application service providers, to ensure the security of all health information on electronic form. Covered entities have to ensure privacy and confidentiality when health information is stored, maintained, or transmitted.

Health plans

A *health plan* is an individual or group plan that provides, or pays the cost of, medical care. Examples of health plans are:

- Group health plans
- Health insurance issuers
- HMOs
- Issuer of Medicare supplemental policies
- Issuers of long term care policies
- Employee welfare benefit plans
- Any other arrangement offering or providing health benefits to the employees of two or more employers
- Government health plans
 - Active military personnel and veterans
 - The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)
 - Indian Health Service
 - Federal Employees Health Benefit Program
 - Approved state child health plans
 - Medicaid + Choice

Health care clearinghouses

Health care clearinghouses are organizations that process health care transactions on behalf of providers and insurers. These include:

- Billing services
- Re-pricing companies
- Medical reviewers
- Community health management information systems
- Value added networks
- Switches

Health care providers

A *health care provider* is a person who is trained and licensed to give health care. A health care provider can also be a place licensed to give health care. Examples of health care providers are:

- Physicians
- Hospitals
- Dentists
- Clinics
- Pharmacies
- Laboratories (all types that serve health care providers)

Scale of impact

The scale of the changes required is staggering. In 2000, there were 10,113 group practices in the U.S having 141,823 physicians and millions of additional staff. According to the Department of Health and Human Services there were 73,125,134 individuals using Medicaid, and many more in private health care programs, not to mention the millions who are not covered by any health plan but are treated through the health care delivery systems.¹

Some of the larger HMOs are shown in the following table.² Physicians, laboratories, non-physician health care professionals all deal with these very large organizations. The specific details of how they address their HIPAA obligations will likely drive the HIPAA compliance schedules of many smaller organizations.

HMO	Medicare + HMO enrollment	Primary + specialty physicians
Anthem BCBS-Anthem HMO, Mason, OH	403,599	16,619
Aetna U.S. Health Care–New Jersey	972,391	15,120
Blue Shield of Calif. Access+HMO	1,123,196	27,054
Health Net of California	2,616,970	35,221
Health Options Inc, Jacksonville, FL	1,132,002	16,780
HIP Health Plan of New York	810,564	15,452
HMO Illinois	984,695	--
Humana Health Plan, Louisville, KY	926,964	NA
Humana Medical Plan, Miramar, FL	709,687	NA
Kaiser Foundation Hlth. Plan/N. Calif.	3,437,027	5,702
Kaiser Foundation Hlth. Plan/S. Calif.	3,330,461	6,474
Keystone Health Plan East	2,616,970	32,258
Keystone Health Plan West	536,772	7,720
Oxford Health Plans–New York	1,112,542	35,012
PacifiCare of Arizona	360,788	4,145
PacifiCare of California	2,779,455	23,473
PacifiCare of Colorado	349,473	4,197
PacifiCare of Texas	568,185	8,301
Regence HMO Oregon, Portland, OR	299,989	6,841
Tufts Health Plan	731,725	17,778
United Health Care–Missouri/St. Louis	560,162	6,668
US Health Care Systems of PA. (Aetna)	843,997	22,698

HIPAA also impacts business associates of the covered entities as well as employers that may in fact be considered a covered entity.

Any program area would almost certainly be impacted if it:

- Receives, submits, or pays health care claims
- Is involved in plan enrollment or benefits
- Receives, distributes or retains patient health care data

Any program may be impacted if it:

- Receives or submits medical information from/to a business partner
- Utilizes information collected from a provider working in a HIPAA compliant environment
- Uses detailed or summary medical information from other entities
- Generates reports from medically related information

In addition, HIPAA may dramatically impact health-related research activities. Health care journal articles report that de-identifying protected health information, acquiring, and managing new consent forms will inject additional labor into an already strained research workforce. They report that this may also cause some physicians and hospitals to reduce the level of their cooperation in order to minimize their potential exposure to HIPAA-related privacy litigation.²

HIPAA timeline

Important dates related to HIPAA compliance are:

- October 16, 2002 — Transactions and Code Sets (extended to October 16, 2003)
- April 16, 2003 — Schedule for testing to begin no later than April 16, 2003
- April 14, 2003 — Privacy
- July 30, 2004 — Employer Identifier
- April 21, 2005 — Security

On December 27, 2001, President Bush signed into law the *Administrative Simplification Compliance Act* (ASCA) (also known as H.R. 3323) delaying the date of compliance for the HIPAA Transaction and Code Set Regulations to October 16, 2003. This date only applies to health plans (except small health plans) and health care providers that submit compliance plans to the Secretary of the Department of Health and Human Services by October 15, 2002.

Under the ASCA, covered entities must submit information on their compliance activities, including budget, assessment of compliance concerns, whether a contractor or vendor might be used to help achieve compliance, and a schedule for testing to begin no later than April 16, 2003.

The HHS model compliance plan involves answering only 26 questions, yet Gartner Group research found that only 65% of providers said that they intended to file this document. Instead, Gartner reports, it appears that these health care organizations are anticipating that their software vendors will provide HIPAA-compliant upgrades that will make the solution simply routine.

For most organizations, this is a high-risk gamble involving a naïve perception that their infrastructure is less complex than it really is. Consider the portions of your organization and its information systems (IS) infrastructure that are impacted by introducing the new HIPAA transaction and code sets. For many, the impact covers a vast array of interfaces, applications, and databases, and likely, some of the processes and procedures that support them. Then consider the time and expense required to perform effective testing and rollout of any of your core, line of business systems. Given the numbers of components of your infrastructure that are likely to change, the testing effort will involve non-trivial time and resource.

Depending on a vendor might be another risk. The vendor might not deliver what you need. One example illustrates the level of vendor commitment on the HIPAA front that Gartner researchers also identified. The author was discussing HIPAA impacts with an agency specializing in collections for health care services organizations. The business's owner believed that his primary systems vendor, Ontario Systems, was still unable (in June of 2002) to provide a coherent and credible explanation of how they were going to deliver HIPAA compliant platforms early enough that his collections agency can perform required testing with each of its customers. Gartner Group researchers found this noncommittal attitude throughout the vendor communities who support health care organizations.

The compliance date for the HIPAA Privacy Rule is set for April 14, 2003. The compliance date for the HIPAA Security Rule is set for April 21, 2005.

Conflict with state law

Section 1178 of HIPAA outlines the relationships between HIPAA's legal and regulatory framework and state law that may address analogous situations or interactions. The general rule is that HIPAA preempts contrary state law. There are three exceptions to this general rule:

- The Secretary of HHS determines that certain state laws are necessary for technical purposes outlined in the statute.
- State laws that the Secretary of HHS determines address controlled substances.
- State laws relating to the privacy of individually identifiable health information that are contrary to and more stringent than the federal requirements.



Do it!

A-1: Discussing HIPAA fundamentals**Questions and answers**

1 Who does HIPAA impact?

HIPAA impacts health plans, health care clearinghouses, and health care providers. These entities have to meet the requirements of HIPAA. Covered entities will need to work with business associates, agents, and contractors that have access to health information to ensure the security of this information in electronic form.

2 How does HIPAA impact covered entities?

HIPAA impacts covered entities by requiring them to ensure privacy and confidentiality when health information is stored, maintained, or transmitted. In addition, specified transactions must comply with HIPAA standards. At a minimum, HIPAA will require covered entities to:

- *Comply with standard transaction sets*
- *Provide information to patients about their privacy rights and how their information can be used*
- *Adopt clear privacy/security procedures*
- *Train employees so that they understand the privacy/security procedures*
- *Designate an individual to be responsible for seeing that the privacy/security procedures are adopted and followed*
- *Secure patient records containing individually identifiable health information so that they are not readily available to those who do not need them*

3 Outline the HIPAA timeline for compliance.

- *October 16, 2002 — Transactions and Code Sets (extended to October 16, 2003)*
- *April 16, 2003 — Schedule for testing to begin no later than April 16, 2003*
- *April 14, 2003 — Privacy*
- *July 30, 2004 — Employer Identifier*
- *April 21, 2005 — Security*

4 Imagine that you're describing HIPAA's core requirements and impact to a client. Summarize the impact HIPAA will have on businesses in the health care industry.

HIPAA will result in:

- *Standardization of electronic, administrative, and financial health care transactions*
- *Unique health identifiers for employers, health plans, health care providers, and eventually individuals*
- *Security standards protecting the confidentiality and integrity of individually identifiable health information, past, present or future*
- *Privacy of protected health information*
- *Standards for electronic medical records*
- *Management burden for compliance project management, execution, testing, training, etc.*
- *Short term expenses to achieve information technology and security compliance*

5 Which of the following are examples of health care providers?

- A** Physicians
- B** Billing services
- C** Hospitals
- D** Medical reviewers
- E** HMOs
- F** Dentists
- G** Pharmacies

6 What is a health care clearinghouse? Give some examples.

Health care clearinghouses are organizations that process health care transactions on behalf of providers and insurers. Examples include:

- ***Billing services***
- ***Re-pricing companies***
- ***Medical reviewers***
- ***Community health management information systems***
- ***Value added networks***
- ***Switches***

Topic B: Administrative Simplification

Explanation

A large section of HIPAA Title II deals with Administrative Simplification. This section of HIPAA is fueling initiatives within organizations to address health care priorities in the areas of transactions, privacy, and security.

HIPAA Title II

HIPAA Title II has seven subtitles:



Subtitle	What it covers
A	Fraud and Abuse Control Program
B	Revisions to Current Sanctions for Fraud and Abuse
C	Data Collection
D	Civil Monetary Penalties
E	Revisions to Criminal Law
F	Administrative Simplification
G	Duplication and Coordination of Medicare-Related Plans

Subtitle F is also called out as Part C in the HIPAA legislation. The focus of this topic will be on the Administrative Simplification subtitle of HIPAA Title II. It is this provision that is the watershed legislation for health care information systems. The purpose of the Administrative Simplification subtitle is to improve the Medicare program under title XVIII of the Social Security Act, the Medicaid program under title XIX of such Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.

HIPAA Administrative Simplification standards

Administrative Simplification was intended to reduce the high cost and administrative burden of health care. Costs would be reduced through the implementation of *Electronic Data Interchange* (EDI) standards for the electronic transmission of many administrative and financial transactions that are predominantly performed on paper. In addition, standards for protecting the privacy and security of patient health information during the transactions will also be implemented.

The following standards (also called rules) mandated by HIPAA will be established by the Secretary of HHS and must be implemented in all health care business applications:

- Standards for Electronic Transactions, also referred to as Transactions, Code Sets and Identifiers
- Standards for Privacy of Individually Identifiable Health Information
- Security and Electronic Signature Standard

HIPAA required the Secretary to adopt standards, when possible, that have been developed by private sector *Standards Development Organizations* (SDOs) accredited by the *American National Standards Institute* (ANSI). These are not government agencies. All of the transactions adopted by this rule are from such organizations. ANSI ASC X12N standards, Version 4010, were chosen for all of the transactions except retail pharmacy transactions, which are from the National Council for Prescription Drug Programs (NCPDP). The choice for the retail pharmacy transactions was the standard maintained by the NCPDP because it is already in widespread use. The NCPDP Telecommunications Standard Format Version 5.1 and equivalent NCPDP Batch Standard Version 1.0 have been adopted in this rule (health plans will be required to support one of these two NCPDP formats).

These standards will be the launch pad for e-business initiatives for electronic, and secure, medical information.

Impact of Administrative Simplification subtitle

The Administrative Simplification subtitle affects health care providers, payers, clearinghouses, billing agents, third-party administrators, and anyone involved exchange of health care information.

Standards for electronic transactions

As mentioned before, health care business applications include patient scheduling, registration, clinical reporting, and billing. Health care business applications are also involved in the storage and movement of medical records and transactions.

Health care transactions are quite varied and include:

- Insurance eligibility verification
- Insurance plan enrollment
- Insurance pre-certification and adjudication
- Scheduling and ordering
- Disease management
- Insurance claims submissions
- Coordination of benefits
- Billing and claims acceptance
- Sharing of patient information between a doctor's office and a hospital

All of these transactions are impacted by HIPAA. Under the Administrative Simplification subtitle of HIPAA, all health care business applications have to be secure and will need to integrate with the health organization's security infrastructure. The intent is to make health care transactions more efficient.

The U.S. GAO estimates that more than 20 cents of every health care dollar is spent on administrative overhead in our health care system.

This overhead is largely driven by billing and administrative costs because of the complexity of transactions involving hundreds of insurers, as shown in Exhibit 1-1.

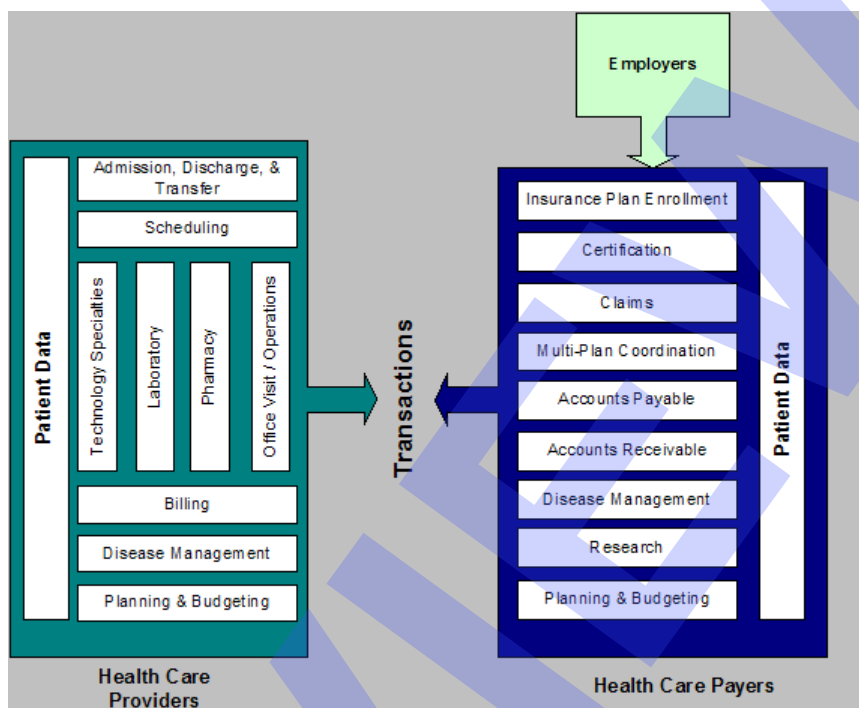


Exhibit 1-1: Health care transactions

The efficiency of information exchange and processing of administrative and financial transactions between health care payers and providers can be greatly improved through the use of computer-to-computer interfaces using EDI transaction standards, which will eliminate human intervention and reduce errors and processing time.

The Administrative Simplification subtitle requires the adoption of EDI transaction standards for certain administrative and financial health care transactions that are currently executed manually (on paper) or electronically without a consistently implemented national standard.

The adoption of transaction standards will also require the implementation of several supporting standards, which will make the implementation of these transaction standards more effective. Currently, payers use hundreds of formats to conduct transactions for claims and payments. The supporting standards include the following:

- Identifiers for plan sponsors (typically employers), health plans, health care providers, and individuals
- Transaction and code sets for diagnosis and procedure codes
- Security and privacy to protect the confidentiality of health information while being stored (data at rest) or transmitted (data in transmission).

The use of EDI combined with stronger security practices will improve health information systems ability to guard against fraud.

Through implementation of strong authentication techniques, access to health information will be better protected. Information systems will be required to automatically log accesses to health information and administrative and financial transactions processed, thus making fraud much more difficult. Together, EDI and stronger security practices will help to make significant reductions in health care costs.



HIPAA Transaction Implementation Guides

The HIPAA Transaction Implementation Guides are published by the Washington Publishing Company (WPC). These guides provide documentation to address industry-specific or company-specific EDI implementation issues, and often include explanatory front matter, figures, examples, and cross-references.

You can download both draft and final versions of HIPAA Implementation Guides in PDF form for free from the WPC Web site:

<http://hipaa.wpc-edi.com/>

You can also order print or CD-ROM copies of the final Implementation Guides.

Available Implementation Guides include:

Title	ANSI ASC X12N standards #
Data Element Dictionary	004010DED
270/271: Health Care Eligibility/Benefit Inquiry and Information Response	004010X092
277/275: Health Care Claim Request for Additional Information and Response	004020X104 & 004020X107 — DRAFT When finalized, this document will be mentioned in an upcoming Notice of Proposed Rulemaking (NPRM).
276/277: Health Care Claim Status Request and Response	004010X093
278: Health Care Services Review — Request for Review and Response	004010X094
820: Payroll Deducted and Other Group Premium Payment for Insurance Products	004010X061
834: Benefit Enrollment and Maintenance	004010X095
835: Health Care Claim Payment/Advice	004010X091
837: Health Care Claim: Institutional	004010X096
837: Health Care Claim: Dental	004010X097
837: Health Care Claim: Professional	004010X098

For additional information about Transaction Standards and HIPAA, visit the U.S. Department of Health and Human Services' Administrative Simplification Web site:

<http://aspe.os.dhhs.gov/admsimp/>

This Web site has information on:

- Identifier standards
- Privacy standards
- Security standards

For information on the Transaction Standard for retail pharmacy claims, visit the National Council for Prescription Drug Programs Web site:

<http://www.ncdp.org>

Privacy and security standards

Privacy and security are addressed separately under HIPAA. Therefore, the standards will be established in two distinct rules. In the context of HIPAA, privacy defines who is authorized to access information and includes the right of individuals to keep information about themselves from being disclosed. Security is defined by the ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss.

Achieving even a base level of this type of security can be harder than one might think. Software, argues John Pescatore, a Gartner Research Vice President, “can be made to do whatever any clever programmer wants it to do; however, it is more difficult to prevent software from doing what you don’t want it to do. Even worse, even if you succeed at that, it is nearly impossible to keep someone else from changing the software to do what you don’t want it to do.”⁴

In a HIPAA-compliant environment where certainty, reliability and carefully-proscribed access to information is key, software’s fluidity, relatively weak self-protection, and constant state of flux can make it an inappropriate foundation for protecting your highest-value information assets. Mr. Pescatore concluded that hardware provides “high levels of security by being more difficult to change than software.” For systems that are relatively stable and must resist modification, he states, “Hardware will be required to provide an appropriate level of security.”⁵

A covered entity can voluntarily choose, but is not required, to obtain the individual’s consent to use and disclose information about him or her for treatment, payment, and health care operations. A covered entity that chooses to have a consent process has complete discretion under the Privacy Rule to design a process that works best for its business and consumers. Health Care Organizations (HCOs) and their business associates will be held accountable for inappropriate disclosures of patient information and will be expected to implement administrative changes to protect information. The Privacy Rule covers the policies and procedures that must be in place to ensure that the patients’ health information is protected and their rights are upheld.

The Security Rule is a companion to the Privacy Rule. In order to protect the information, HCOs will be expected to put in place security safeguards. Complementing the Security Rule, the HIPAA Privacy Rule defines who is authorized to access patient-identifiable information. It also will establish the rights of individuals to keep information about them from being disclosed.

The provisions of the Privacy Rule overlap with the Security Rule in some areas. For instance, the final Security Rule requires that health care organizations conduct an information system activity review on a regular basis.

Businesses will need the assistance of skilled security professionals and architects for a successful implementation of HIPAA-related security assessment, policies, and technologies.

Secure information delivery

Traditionally, the health care industry has been impeded by:

- Limited technology budgets
- Multiple proprietary systems
- Multiple legacy systems
- Paper-based processes

The mandated HIPAA regulations are the catalyst to improve processes and information flow throughout the health care industry. The Administrative Simplification subtitle includes provisions to help secure information delivery between administrators, patients and caregivers. These provisions address the electronic capture, transformation and delivery of health care information across the health care industry entities.

As a direct consequence of health care transactions, it is becoming much more important to protect patient and medical information. This requires the health care organization to build a secure infrastructure.

The key components of a secure infrastructure for a health care organization may include the deployment of technologies such as:

- Firewall systems
- Intrusion Detection Systems (IDS)
- Secure Virtual Private Networks (VPNs)
- Public Key Infrastructure (PKI)
- Biometrics
- Smart cards
- Authentication tokens

Thus, the HIPAA-compliant health care organization is one that would use EDI for transactions, protect patient's medical information with a combination of notices, consents, and authorization and secure all electronic medical records and transactions. The result is e-business being implemented by the health care industry.

Do it!

B-1: Discussing Administrative Simplification

Questions and answers

1 Let's say your client wants to better understand HIPAA Administrative Simplification standards. What are the key standards and supporting standards that will be adopted?

The Administrative Simplification standards include:

- *Standards for Electronic Transactions, Code Sets, and Identifiers*
- *Standards for Privacy of Individually Identifiable Health Information*
- *Security and Electronic Signature Standards*

Supporting standards include:

- *Standards for Code Sets*
- *National Standard for Identifiers*

2 Why is HIPAA fundamentally about e-business initiatives within an organization?

Because health care business applications include patient scheduling, registration, clinical reporting, and billing. Health care business applications are also involved in the storage and movement of medical records and transactions. The Administrative Simplification subtitle specifies that standards be adopted for the implementation of Electronic Data Interchange (EDI) standards for the electronic transmission of many administrative and financial transactions that are predominantly performed on paper. In addition, standards for protecting the privacy and security of patient health information during the transactions will also be implemented.

As a result of HIPAA, all health care business applications have to be secure and will need to integrate with the health organization's security infrastructure. These standards will be the launch pad for e-business initiatives for electronic, and secure, medical information.

3 After listening to a quick executive overview of HIPAA basics, your client asks for examples of some specific and relevant “transactions.” What might you include in this list of examples?

A transaction amounts to the exchange of information between two parties to carry out health care financial or administrative activities. There are transactions that cover the following types information exchanges:

- **Health claims or equivalent encounter information**
- **Health care payment and remittance advice**
- **Coordination of benefits**
- **Health claims status**
- **Enrollment and disenrollment in a health plan**
- **Eligibility for a health plan**
- **Health plan premium payments**
- **Referral certification and authorization**
- **First report of injury**
- **Health claims attachments**
- **Other transactions that the Secretary of HHS may prescribe by regulation**

4 Identify some key technology components of a secure infrastructure for a health care organization.

- **Firewall systems**
- **Intrusion Detection Systems (IDS)**
- **Secure Virtual Private Networks (VPNs)**
- **Public Key Infrastructure (PKI)**
- **Biometrics**
- **Smart cards**
- **Authentication tokens**

Topic C: HIPAA penalties

Explanation

HIPAA sets severe penalties for noncompliance. The penalties may be either civil or criminal. In addition, some penalties are financial, while others might include imprisonment.

Violation of HIPAA requirements

For example, penalties for violation of patient confidentiality standards are substantial with monetary fines and in some cases imprisonment. Under the Administrative Simplification subtitle, section 1176, says that the Secretary of HHS can impose a civil monetary fine on any person or covered entity that violates any HIPAA requirement. The civil monetary penalty for violating transaction standards is up to \$100 per person per violation and up to \$25,000 per person per violation of a single standard per calendar year.

The Secretary of HHS can reduce the amount of a fine or waive it entirely if the violation was not due to willful neglect of the requirements, and if the entity corrects it within 30 days of becoming aware of it.

Federal criminal penalties can also be placed upon health plans, providers, and health care clearinghouses that knowingly and improperly disclose information or obtain information under false pretenses. Penalties would be higher for actions designed to generate monetary gain.

In addition, HIPAA also establishes penalties for a knowing misuse of unique health identifiers and individually identifiable health information:

- A fine of not more than \$50,000 and/or imprisonment of not more than 1 year
- If misuse is under false pretenses, a fine of not more than \$100,000 and/or imprisonment of not more than 5 years
- If misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than \$250,000 and/or imprisonment of not more than 10 years.

The specific offenses to which harsher penalties apply include:

- Using a unique health identifier in violation of the HIPAA requirements. Unique health identifiers include:
 - Provider identifiers
 - Employer identifiers
 - Health plan identifiers
 - Individual identifiers
- Obtaining or using individually identifiable health information in violation of the HIPAA privacy requirements
- Disclosing individually identifiable health information in violation of the HIPAA privacy requirement

The following table summarizes HIPAA civil penalties.

Monetary penalty	Terms of imprisonment	Offenses
\$100	N/A	Single violation of a provision (can be multiple violations with penalty of \$100 each as long as each violation is for a different provision)
\$25,000	N/A	Multiple violations of an identical requirement or prohibition made during a calendar year

The following table summarizes HIPAA criminal penalties.

Monetary penalty	Terms of imprisonment	Offenses
Up to \$50,000	Up to one year	Wrongful disclosure of individually identifiable health information
Up to \$100,000	Up to five years	Wrongful disclosure of individually identifiable health information committed under false pretenses
Up to \$250,000	Up to ten years	Wrongful disclosure of individually identifiable health information committed under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm

In addition to significant financial penalties, remaining non-compliance might result in the additional consequences:

- Claims not honored
- Bad press
- Legislative auditors

Who can file a complaint?

Any person who believes that a provider, health plan, or clearinghouse has not complied with HIPAA's provision may file a complaint.

Window for filing a complaint

The complaint must be filed within 180 days of the time the person filing the complaint became aware of a HIPAA violation.

Who can be penalized?

The HIPAA penalties apply to covered entities. Senior individuals within covered entities may be punished for non-compliance. A senior manager who is aware of a violation cannot avoid responsibility by avoiding active participation.

A covered entity is liable for violations of HIPAA requirements by its:

- Employees
- Other members of its workforce
- Business associates

A covered entity must establish and apply sanctions to members of its workforce who fail to comply with HIPAA's privacy and security policies and requirements. It must also maintain records of any sanctions that are applied and is obligated to make those records available to the Secretary, when requested, during the investigation of any complaint.

At a minimum, HIPAA will require:

- Compliance with standard transaction sets
- Providing information to patients about their privacy rights and how their information can be used
- Adopting clear privacy/security procedures
- Training employees so that they understand the privacy/security procedures
- Designating an individual to be responsible for seeing that the privacy/security procedures are adopted and followed
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them

HHS Secretary authorization

The HHS Secretary is authorized to launch a compliance review of a covered entity whether or not a complaint alleging a violation of HIPAA's provisions has been received.

Effective date of penalties

The earliest date of an infraction that will be subject to HIPAA's penalty provision is April 14, 2003.

Do it!

C-1: Discussing HIPAA penalties

Questions and answers

1 What type of penalties does HIPAA set for noncompliance?

HIPAA sets severe penalties for noncompliance. The penalties may be civil or criminal. Penalties might take the form of monetary fines or imprisonment.

2 Give some examples of criminal penalties under HIPAA.

Criminal penalties are:

- *Up to \$50,000 and one year in prison for obtaining or disclosing protected health information*
- *Up to \$100,000 and up to five years in prison for obtaining protected health information under false pretenses*
- *Up to \$250,000 and up to ten years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm*

3 What is the civil monetary penalty for violating transaction standards?

The civil monetary penalty for violating transaction standards is up to \$100 per person per violation and up to \$25,000 per person per violation of a single standard per calendar year.

4 What is the penalty for misuse with intent to sell, transfer, or use identifiable health information?

If misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than \$250,000 and/or imprisonment of not more than 10 years.

Topic D: HIPAA-related organizations

Explanation

In this topic we review some organizations closely associated with the HIPAA legislation.

U.S. Department of Health and Human Services (HHS)

One of the largest federal agencies, the Department of Health and Human Services (HHS) is the principal agency for protecting the health of all Americans. Comprising 12 operating divisions, HHS' responsibilities include public health, biomedical research, Medicare and Medicaid, welfare, social services, and more. An overview of the department is provided in the document "HHS: What We Do," which you can download from:

www.hhs.gov/about/profile.html

Centers for Medicare and Medicaid Services (CMS)

The *Centers for Medicare and Medicaid Services* (CMS) provides health insurance for over 74 million Americans through Medicare, Medicaid and State Children's Health Insurance Program (SCHIP). This federal government agency was previously known as the Health Care Financing Administration (HCFA).

In addition to providing health insurance, CMS also performs a number of quality-focused activities, including regulation of laboratory testing, development of coverage policies, and quality-of-care improvement. CMS maintains oversight of the survey and certification of nursing homes and continuing care providers (including home health agencies, intermediate care facilities for the mentally retarded, and hospitals), and makes available to beneficiaries, providers, researchers and State surveyors information about these activities and nursing home quality.

HIPAA is an initiative of the Department of Health and Human Services/CMS. CMS is responsible for implementing the various unrelated provisions of HIPAA. CMS's business activities with regard to HIPAA include:

- HIPAA Health Insurance Reform
- HIPAA Administrative Simplification

For further information, go to the CMS Web site:

www.cms.hhs.gov

Designated Standards Maintenance Organization (DSMO)

The Secretary of HHS named six organizations to maintain the standards using criteria specified in the Privacy and Security Rules. These organizations are referred to as *Designated Standards Maintenance Organizations* (DSMOs). They are:

- ANSI Accredited Standards Committee (ASC) X12
- Dental Content Committee of the American Dental Association
- Health Level Seven (HL7)
- National Council for Prescription Drug Programs (NCPDP)
- National Uniform Billing Committee (NUBC)
- National Uniform Claim Committee (NUCC)

For further information, go to the DSMO Web site:

www.hipaa-dsmo.org

Workgroup for Electronic Data Interchange (WEDI)

The *Workgroup for Electronic Data Interchange* (WEDI) was established in 1991 to address administrative costs in the nation's health care system. WEDI is a voluntary, public/private task force created to streamline health care administration by standardizing electronic communication across the industry.

The mission of WEDI includes serving as the primary catalyst for the identification, communication and resolution of obstacles that impede the growth of electronic commerce within health care.

WEDI members have included Blue Cross Blue Shield Association, Travelers Insurance, and many others.

For further information, go to the WEDI Web site:

www.wedi.org

Health Level Seven (HL7)

Health Level Seven (HL7) standards are widely used to interface the independent systems in health care institutions concerned with clinical information. HL7 became an ANSI-accredited Standards Developing Organization (SDO) in 1994. HL7's involvement with HIPAA has been with claims attachments.

There are several HL7 documents, including those that cover:

- Ambulance
- Clinical reports
- Emergency department
- Laboratory results
- Medications
- Rehabilitation services

For further information, go to the HL7 Web site:

www.hl7.org



Washington Publishing Company (WPC)

The Washington Publishing Company (WPC) specializes in managing and distributing Electronic Data Interchange (EDI) information, primarily in the form of documentation for organizations that develop, maintain, and implement EDI standards.

The EDI subsets, called Implementation Guides, also address industry-specific or company-specific EDI implementation issues, and often include explanatory front matter, figures, examples, and cross-references. WPC has published several EDI Implementation Guides for several industries including:

- Association of American Railroads (AAR)
- American Trucking Association (ATA)
- Information System Agreement
- Telecommunications Information Forum
- Petroleum Industry Data Exchange
- Book Industry Systems Advisory Committee (BISAC)
- Serials Industry Systems Advisory Committee (SISAC)
- Automotive Industry Action Group (AIAG)
- National Association of Purchasing Managers (NAPM)
- American Iron and Steel Institute (AISI)
- Aluminum Association

For further information, go to the WPC Web site:

www.wpc-edi.com

National Council for Prescription Drug Programs (NCPDP)

The *National Council for Prescription Drug Programs* (NCPDP) first started developing standards in 1977 with the Universal Claim Form. Transactions between pharmacies and health plans are typically executed in the NCPDP standard, while the transactions between all other providers and plans are done with X12 standards.

For Health Care Eligibility Benefit Inquiry and Response as well as Health Care Payment and Remittance Advice, the standard transaction for retail pharmacy drugs is the NCPDP Telecommunication Standard for Eligibility Verification and Response and Enrollment. The NCPDP's Telecommunication Standard processes over 1 billion claims per year. NCPDP received ANSI accreditation status in 1996.

NCPDP is a not-for-profit organization. Its target audience includes the pharmacy services sector of the health care industry. This includes organizations such as:

- Pharmacy chains
- Database management organizations
- Pharmaceutical manufacturers
- Telecommunication and systems vendors
- Wholesale drug distributors

For further information, go to the NCPDP Web site:

www.ncdp.org



National Committee on Vital and Health Statistics (NCVHS)

The *National Committee on Vital and Health Statistics* (NCVHS) is an advisory committee to the Secretary of Health and Human Services.

The HIPAA Administrative Simplification Compliance Act (ASCA) requires that a sample of the plans be provided to NCVHS. The NCVHS will review the sample to identify common problems that are complicating compliance activities, and will periodically publish recommendations for solving the problems.

For further information, go to the NCVHS Web site:

www.ncvhs.hhs.gov

Do it!

D-1: Discussing HIPAA-related organizations

Questions and answers

1 What is the target audience of the NCPDP?

NCPDP's target audience includes the pharmacy services sector of the health care industry. This includes organizations such as:

- *Pharmacy chains*
- *Database management organizations*
- *Pharmaceutical manufacturers*
- *Telecommunication and systems vendors*
- *Wholesale drug distributors*

2 What do WPC published Implementation Guides address?

These guides generally address industry-specific or company-specific EDI implementation issues, and often include explanatory front matter, figures, examples, and cross-references.

3 Describe the NCVHS organization. How is the NCVHS involved with the HIPAA ASCA?

The National Committee on Vital and Health Statistics (NCVHS) is an advisory committee to the Secretary of Health and Human Services. The HIPAA Administrative Simplification Compliance Act (ASCA) requires that a sample of the plans be provided to NCVHS.

4 What is the purpose of a DSMO? Give some examples of specific DSMOs.

The Secretary of HHS named six organizations to maintain the standards using criteria specified in the Rules defined. These organizations are referred to as Designated Standards Maintenance Organizations (DSMOs). They are:

- *ANSI Accredited Standards Committee (ASC) X12*
- *Dental Content Committee of the American Dental Association*
- *Health Level Seven (HL7)*
- *National Council for Prescription Drug Programs (NCPDP)*
- *National Uniform Billing Committee (NUBC)*
- *National Uniform Claim Committee (NUCC)*

Topic E: HIPAA terminology

Explanation

The HIPAA legislation uses specific terminology that needs to be understood when considering the impact and breadth of the law.

Covered entities

The regulations place specific obligations upon covered entities. Covered entities include payers and providers. Payers include health plans (including most employer-sponsored group health plans), health care clearinghouses. Providers include any health care provider who transmits any health information in electronic form in connection with (regulated health care claims administration and financial transactions with payers).

Most health care providers use electronic transmission in some form or the other when processing claims or in their financial dealings with their payers, such as with Medicare or commercial plans. These regulations, thus, will apply to most health care providers.

In today's health care system, however, most health care providers and payers do not independently carry out all their health care activities and functions. They require assistance from a variety of service providers and contractors. HIPAA describes these supporting entities as business associates.

Health plans

Health plans are considered covered entities. These include employee welfare benefit plans under Employee Retirement Income Security Act (ERISA), including insured and self-insured plans, that have 50 or more participants or which are administered by an entity other than the employer that establishes and maintains the plan.

Health plans under the regulations also include a health insurance issuer, an HMO, the Medicare and Medicaid programs, as well as most all federal health care programs, issuers of long-term care policies, and any other individual or group plan (or combination of individual or group plans) that provides or pays for the cost of medical care.

Health plans include the following, singly or in combination:

Plan	Description
Group Health Plan	A plan that has 50 or more participants or is administered by an entity other than the employer that established and maintains the plan. This definition includes both insured and self-insured plans.
Health Insurance Issuer	An insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance.
Health Maintenance Organization (HMO)	May include preferred provider organizations, provider sponsored organizations, independent practice associations, competitive medical plans, exclusive provider organizations, and foundations for medical care.
Medicare	Part A or Part B of the Medicare program (title XVIII of the Act).
Medicaid	The Medicaid program (title XIX of the Act).

Plan	Description
Medicare Supplemental Policy	A health insurance policy that a private entity offers a Medicare beneficiary to provide payment for expenses incurred for services and items that are not reimbursed by Medicare because of deductible, coinsurance, or other limitations under Medicare. The statutory definition of a Medicare supplemental policy excludes a number of plans that are generally considered to be Medicare supplemental plans, such as health plans for employees and former employees and for members and former members of trade associations and unions.
Long Term Care Policy	Includes nursing home fixed-indemnity policies, and is considered to be a health plan regardless of how comprehensive it is.
Employee Welfare Benefit Plan	A plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers. This includes plans that are referred to as Multiple Employer Welfare Arrangements (MEWAs).
Active Military Personnel Health Plan	The health care program for active military personnel under title 10 of the United States Code.
Veterans Health Care Program	The health care program under chapter 17 of title 38 of the United States Code. This health plan primarily furnishes medical care through hospitals and clinics administered by the Department of Veterans Affairs for veterans with a service-connected disability that is compensable. Veterans with non service-connected disabilities (and no other health benefit plan) may receive health care under this health plan to the extent resources and facilities are available.
CHAMPUS	The Civilian Health and Medical Program of the Uniformed Services. CHAMPUS primarily covers services furnished by civilian medical providers to dependents of active duty members of the uniformed services and retirees and their dependents under age 65.
Indian Health Service	Furnishes services, generally through its own health care providers, primarily to persons who are eligible to receive services because they are of American Indian or Alaskan Native descent.
Federal Employees Health Benefits Program	Consists of health insurance plans offered to active and retired federal employees and their dependents. Depending on the health plan, the services may be furnished on a fee-for-service basis or through a health maintenance organization.
State Child Health Plan	An approved health plan under Title XXI of the Act, providing benefits that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397 et. Seq.
Medicare + Choice	The Medicare + Choice program under part C of Title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
Other	Any other individual or group health plan, or combination thereof, that provides or pays for the cost of medical care.

Health care clearinghouse

The term *health care clearinghouse* refers to any public or private entity that:

- Processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or standard transactions
- or—
- Receives a standard transaction from another entity and processes or facilitates the processing of information into nonstandard format or nonstandard data content for a receiving entity

A health care clearinghouse is an entity that performs the functions of format translation and data conversion. When they are engaged in these activities, a billing service company, re-pricing company, community health management information system or community health information system, or value-added networks and switches, would be considered a health care clearinghouse.

Health care industry businesses of a threshold size have used software data and transaction mapping tools to convert Electronic Data Interchange (EDI) transactions between their external exchange formats and the internal core system-specific formats. Over time, some of these systems matured into sophisticated transaction brokers, or were built upon one of the commercial transaction brokers. The new HIPAA transactions cause owners of these “older,” often highly customized or proprietary gateways, to make a difficult decision: Should we rewrite or otherwise extend my existing transaction switch, or purchase one of the new commercial *switches* that are emerging in the health care support services market?

Another way to view these EDI/transaction switches, is to view them as high-level middleware. Gartner Group calls these systems *Integration Brokers* (IBs). They describe the new family of transaction switches as facilitating “communication among different applications by negotiating a variety of native data formats and communication protocols, and help ensure the timely and reliable delivery of messages from one application to another.”

A number of vendors are marketing specialized HIPAA supporting transaction switches. These systems include pre-configured mappings for the HIPAA transactions. Some of the leading vendors that support HIPAA-related transaction products and solutions include:

- IBM
- Mercator
- Microsoft
- Optio
- SeeBeyond
- Sybase
- TIBCO
- Vitria



Health care provider

Regulations define a *health care provider* as limited to those entities that furnish, or bill and are paid for, health care services in the normal course of business.

Health information

Health information means any information, whether oral or recorded in any form or medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual

Individually Identifiable Health Information (IIHI)

The concept of what information constitutes individually identifiable health information and what information may be protected health information are important in order to understand the obligations placed upon covered entities by the privacy regulations. Individually identifiable health information includes that health information, including demographic information collected from an individual, that:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse
- Relates to the past, present, or future physical or mental health or condition of an individual
- Relates to the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual
- Identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual

Patient Identifiable Information (PII)



The term *Patient Identifiable Information (PII)* refers to identifiers within health information that could be used to identify an individual. This may include any one of the following:

- The individual's name
- The city or county in which the individual lives
- Zip Code
- Social security number
- Fingerprint
- Telephone number
- Medical record number or fax number

The regulations list a number of other identifiers. Thus, any health information maintained by a covered entity where the individual could, in any possible way, be identified, needs to be treated as individually identifiable health information.

Business associate

These regulations also place requirements on covered entities when they disclose protected health information to their business associates. A *business associate* of a covered entity is generally a person (other than a member of its workforce) that, on behalf of the covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and re-pricing.

It also includes persons (other than members of the covered entity's work force) that provide legal, actuarial, accounting consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity to the person(s).

Exceptions to the definition apply to the arrangements between participants in certain joint health care arrangements.

Providers and payers are able to give protected health information to business associates, but they must:

- Ensure that the business associate will use the information only for the purpose for which they were engaged by the covered entity
- Safeguard the information from misuse
- Comply with the covered entity's obligation to provide individuals with access to their health information and history of certain disclosures
- Never use protected health information for any purpose independent of their explicit responsibilities to the contracting covered provider or payer

Given the broad definition of business associates, covered entities will need to carefully consider how these regulations may apply to anyone with whom they contract, when that arrangement may result in the disclosure of individually identifiable health information.

Four business associate exceptions involve treatment, financial transactions, disclosures, between a group health plan and plan sponsor, and organized health care arrangements.

Small health plan

A *small health plan* is one with annual receipts of \$5 million or less. A small health plan is typically an individual health plan or group health plan with fewer than 50 participants.

Participant

A *participant* is any employee, or former employee of an employer or any member of former member of an employee organization who is or may be eligible to receive a benefit of any type from an employee benefit plan that covers employees of that employer or members of such or organization, or whose beneficiaries may be eligible to receive any of these benefits.

Medical care

Medical care includes the diagnosis, cure, mitigation, treatment, and prevention of disease or amounts paid for the purpose of affecting any body structure or function of the body. It also includes the amount paid for transportation primarily for and essential to the items identified. Finally, it includes the amount paid for insurance to cover the items as well as the transportation of all such items.

Secretary

The Secretary is the Secretary of the Department of Health and Human Services or any other officer or employee of the Department of Health and Human Services to whom the authority involved has been delegated.

Compliance date

The *compliance date* is the latest date by which a covered entity such as a health plan, health care clearinghouse, or health care provider must comply with a rule. The compliance date for HIPAA standards generally is 24 months after the effective date of a final rule. The compliance date for small health plans, however, is 36 months after the effective date of the final rule.

Transaction

A *transaction* is the exchange of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information exchanges:

- Health claims or equivalent encounter information
- Health care payment and remittance advice
- Coordination of benefits
- Health claims status
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization
- First report of injury
- Health claims attachments
- Other transactions that the Secretary may prescribe by regulation

In general, a health plan must conduct the above transaction electronically when requested by a provider or another entity.

A transaction consists of code sets and identifiers.



Data content

Data content includes the *data elements* and *code sets* inherent to a transaction and not related to the format of the transaction. Data elements that are related to the format are not data content.

Data issues will impact both payers and providers. HIPAA transactions introduce new data elements, and revised lengths for other data elements. For example, HIPAA standards introduce a new system of identifiers for providers and health plans. When used to describe a transaction, format refers to those data elements that structure it, or assists in identifying its data content.

Transaction standard

A *transaction standard* is a set of rules, conditions, or requirements describing the classification and components of a transaction. Transaction standards define the data elements, code sets, and details of inter-system interactions that must be used in a transaction.

The transaction standard will likely require that some insurance providers to invest in relatively complex application and/or interface development to support some of its more intrusive requirements.

For example, even though it is common practice to “bundle” remittance advice, HIPAA compliance requires that remittance advice must be expressed using the same record of services that were submitted in the corresponding claim. Depending on the state of a given insurer’s systems, this new business-to-business interaction logic will require more or less coding, testing, documentation, training, and project management.

Code set

Code set means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

Trading partner agreement



A *trading partner agreement* is an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement.

For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.

Specifically, trading partner agreements must NOT:

- Modify the definition, condition, or use of a data element or segment in the standard Implementation Guide
- Add any additional data elements or segments to the Implementation Guide
- Utilize any code or data values, which are not valid in the Implementation Guide
- Change the meaning or intent of the Implementation Guide

Workforce

The term *workforce* refers to employees, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity.

Long-term care

Long-term care refers to the range of services typically provided at skilled nursing, intermediate-care, personal care, or eldercare facilities.

Organized Health Care Arrangement (OHCA)

An *Organized Health Care Arrangement* (OHCA) is a clinically integrated setting in which patients receive care from multiple health care providers. Providers participating in an organized health care arrangement are not business associates of each other. Examples include independent practice associations of physicians and hospital medical staff arrangements.

Patient event

The term *patient event* refers to the service or group of services associated with a single episode of care. Examples include:

- An admission to a facility for treatment related to a specific patient condition or diagnosis or related group of diagnoses
- A referral to a specialty provider for a consult or testing to determine a specific diagnosis and appropriate treatment
- Services to be administered at a patient visit such as chiropractic treatment delivered in a single patient visit (The same treatment can be approved for a series of visits. It is recommended by the ANSI ASC X12N standard to limit each request to a single patient event.)

Requester

A *requester* is a provider such as physicians, medical groups, independent physician associations, facilities, and others who request authorization or certification for a patient to receive health care services.

Service provider

A *service provider* is the referred-to provider, specialist, specialty entity, group, or facility where the requested services are to be performed.

Utilization Management Organization (UMO)

A *Utilization Management Organization* (UMO) is an insurance company, HMO, Preferred Provider Organization (PPO), health care purchaser, professional review organization, other provider, or other utilization review entity that receives and responds to requests for authorization and certification.

The UMO may or may not be the organization that makes the medical decision on a service review request. The UMO might have a relationship with a payer that calls for the payer to make a decision in certain cases. It is the role of the UMO to forward that request to the payer, receive the response from the payer, and then return the response to the requester.

From the requester's perspective, the exchange of information is between the requester and the UMO.

Do it!

E-1: Discussing HIPAA terminology

Questions and answers

- 1 Let's say your client wants to better understand exactly what constitutes covered entities under HIPAA legislation. Describe the scope of covered entities under HIPAA.

The regulations place specific obligations upon covered entities. Covered entities include health plans (including most employer-sponsored group health plans), health care clearinghouses, and any health care provider who transmits any protected health information in electronic form in connection with regulated health care claims administration and financial transactions with payers.

Most health care providers use electronic transmission in some form or the other when processing claims or in their financial dealings with their payers, such as with Medicare or commercial plans. These regulations, thus, will apply to most health care providers.

- 2 What is a health care clearinghouse?

A health care clearinghouse is an entity that performs the functions of format translation and data conversion. When they are engaged in these activities, a billing service company, re-pricing company, community health management information system or community health information system, or value-added networks and switches, would be considered a health care clearinghouse.

- 3 Give some examples of identifiers within health information that constitute patient identifiable information?

- *The individual's name*
- *City or county where the individual lives*
- *Zip Code*
- *Social security number*
- *Finger print*
- *Telephone number*
- *Medical record number or fax number*

- 4 What does UMO refer to?

Utilization Management Organizations (UMOs) are insurance companies, HMOs, Preferred Provider Organizations (PPO), health care purchasers, professional review organizations, other providers, and other utilization review entities that receive and respond to requests for authorization and certification.

- 5 Define the term "business associate."

A business associate is defined as a person or company that provides a service that requires their use of PHI. PHI includes patient demographic information, claims data, insurance information, diagnostics information, and any other information that relates to the past, present, or future health condition, provision of health care, payment for health care and that identifies the individual (or reasonable reason it could identify the individual).

- 6 Should a hospital's board of directors sign business associate agreements? Why or why not?

This is not an easy one. Board members may have access to PHI when QA and other patient issues reach the board level. They may not be business associates because they are the entity. The workforce definition does not apply to board members because they are not individuals under the direct control of the entity. However, board members do set policy and strategy for the organization and may review PHI from time-to-time. So while they may not be employees, they do represent the entity.

- 7 A hospital contracts with a bank to process credit card payments by its patients for health care services. Is the bank a business associate? Why or why not?

The bank is not a business associate of the hospital. The reason is that no business associate agreement is required between a covered entity and a financial institution if it only processes consumer-conducted financial transactions in payment for health care.

- 8 A hospital uses a courier service to deliver medical records to a laboratory. Is the courier service a business associate? Why or why not?

The courier service is not a business associate of the hospital because it does not have access to PHI.

- 9 Would a hospital's Internet Service Provider (ISP) require a business associate agreement? Why or why not?

This depends on whether they access PHI in the course of their normal duties. If they do then a business associate agreement would be a requirement.

- 10 Would a cleaning service vendor require a business associate agreement? Why or why not?

If the cleaning services company is not under the direct control of the covered entity they may qualify for a business associate agreement.

- 11 Who are the exceptions to the business associate rules?

Four business associate exceptions involve treatment, financial transactions, disclosures between a group health plan and plan sponsor, and organized health care arrangements.

- 12 Describe an organized health care arrangement. Are participating providers required to have business associate agreements between them? Explain.

An organized health care arrangement is a clinically integrated setting in which patients receive care from multiple health care providers. Providers participating in an organized health care arrangement are not business associates of each other. Examples include independent practice associations of physicians and hospital medical staff arrangements.

Unit summary: HIPAA basics

- Topic A** In this unit, you learned that **HIPAA** is the **Health Insurance Portability and Accountability Act of 1996**. You also learned about the motivation drivers for the HIPAA legislation. HIPAA has five **titles**. The core component of the HIPAA legislation that impacts **electronic transactions** within health care organizations is Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform. You learned that HIPAA will impact **health plans, health care clearinghouses, and health providers**. You also learned the **timelines** for HIPAA compliance.
- Topic B** Next, you learned more about the HIPAA **Administrative Simplification** subtitle. This section of HIPAA is fueling initiatives within organizations to address health care priorities in the areas of **transactions, privacy, and security**. The Administrative Simplification subtitle calls for **Electronic Data Interchange (EDI)** standards for the electronic transmission of many administrative and financial transactions that are predominantly performed on paper. In addition, standards for protecting the privacy and security of patient **health information** during the transactions will also be implemented. The Administrative Simplification standards will include: standards for electronic transactions; standards for code sets; a national standard for identifiers; standards for privacy of individually identifiable health information; and security standards.
- Topic C** Then, you learned that HIPAA has real **penalties and timelines** associated with it. More so than just a legislative requirement, all **entities** need to examine how the application of HIPAA requirements will improve **business processes, communications and systems**.
- Topic D** Next, you learned that there are number of **organizations** associated with the HIPAA legislation. Most of these organizations work closely with the **Department of Health and Human Services (HHS)** in coordinating and managing several aspects of the legislation. Some of the organizations you learned about include **CMS, DSMO, WEDI, WPC, NCPDP, and NCVHS**.
- Topic E** Finally, you learned some of the key **terminology** related to the HIPAA legislation. You learned how to identify **covered entities** such as **health plans, health care clearinghouses, and health providers**. You also learned what constitutes a business **associate**. Then you learned about **health information, individually identifiable health information, and patient identifiable information**. You also learned about **transactions, data content, transaction standards, and code sets**.

Review questions

- 1 The definition of the term *workforce* is important in the context of identifying business associates. Define this term.

The term workforce refers to employees, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity.

- 2 What is health information?

Health information is any information, whether oral or recorded in any form or medium, that:

- *Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse*
- *Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual*

- 3 Identify some vendors that support HIPAA-related transactions products and solutions.

- *IBM*
- *Mercator*
- *Microsoft*
- *Optio*
- *SeeBeyond*
- *Sybase*
- *TIBCO*
- *Vitria*

- 4 What should trading partner agreements not result in?

Specifically, trading partner agreements must NOT:

- *Modify the definition, condition, or use of a data element or segment in the standard Implementation Guide*
- *Add any additional data elements or segments to the Implementation Guide*
- *Utilize any code or data values that are not valid in the Implementation Guide*
- *Change the meaning or intent of the Implementation Guide*

- 5 Give two examples of Organized Health Care Arrangements (OCHAs)?

Examples of OCHA include independent practice associations of physicians and hospital medical staff arrangements.

Endnotes

#	Reference
1	“Care Delivery Organization Financial and Administrative Application Study: 2002 Results.” 12 June 2002, by Michael Davis, Randy Dearborn, & Tom Berg. Gartner Group Note Number: R-17-0375. http://www.managedcaredigest.com/edigests/mg2001/mg2001c01s1ag02.shtml ; http://www.hcfa.gov/medicaid/omc2001.htm
2	Interstudy data quoted in “Top 25 HMOs Ranked by Medicare Enrollment.” (as of 01/01/2002) by Jean M. Appleby, Managed HealthCare Executive. June 2000, p. 52; and Aventis Managed Care Digest Series at: http://www.managedcaredigest.com/edigests/hm2000/hm2000.html .
3	See “April 2002 HIPAA Panel Results: Deadline Extension Impact.” 10 June 2002, by Matthew Duncan, Gartner Group Note Number: QA-16-9213
4	“Software Security Is Soft Security: Hardware Is Required.” by John Pescatore, 10 June 2002, Gartner Group Note Number: COM-16-5309, http://www4.gartner.com/DisplayDocument?id=359830