HCPro

Omnibus Rule Update

HIPAA Handbook for Healthcare Staff

Understanding the Privacy and Security Regulations

Kate Borten, CISSP, CISM

HIPAA Handbook for Healthcare Staff

Understanding the Privacy and Security Regulations

HCPro

HIPAA Handbook for Healthcare Staff: Understanding the Privacy and Security Regulations is published by HCPro, Inc.

ISBN: 978-1-61569-228-6

Kate Borten, CISSP, CISM, Author
Gerianne Spanek, Managing Editor
Mary Stevens, Editor
James T. DeWolf, Publisher and Editorial Director
Mike Mirabello, Production Specialist
Adam Carroll, Proofreader
Matt Sharpe, Senior Manager of Production
Shane Katz, Art Director
Jean St. Pierre, Vice President of Operations and Customer Service

Advice given is general. Readers should consult professional counsel for specific legal, ethical, or clinical questions. Arrangements can be made for quantity discounts. For more information, contact:

HCPro, Inc.
75 Sylvan Street, Suite A-101
Danvers, MA 01923
Telephone: 800-650-6787 or 781-639-1872
Fax: 800-639-8511
Email: *customerservice@hcpro.com*

Visit HCPro online at *www.hcpro.com* and *www.hcmarketplace.com.*

05/2013
22025

CONTENTS

About the Author vi

Intended Audience 1

Learning Objectives 2

HIPAA Basics 3

HITECH Act and Omnibus Rule Overview 3

HIPAA and You 3

Terms You Should Know 4

- Covered entities 4
- Protected health information or PHI 4
- Minimum necessary/need to know 6
- Examples of using minimum necessary and need-to-know standards 6
- Case scenario #1: Celebrity sighting 7

Privacy 9

- Use and release of PHI 9
- What your facility does to protect confidentiality 10
- What you can do to protect confidentiality 11
- Case scenario #2: Patients and their family members 11
- Case scenario #3: Good intentions 12

Case scenario #4: Sometimes you need to vent 13

Faxing 14

Case scenario #5: "Hello, Pete's Plumbing, how may I help you?" 15

Discarded patient information 15

Patient directory 16

Incidental disclosures 16

High-risk situations: Elevators, lobbies, and other public places 16

High-risk situations: Printouts 17

High-risk situations: Friends and family 17

High-risk situations: Your friends and family 17

Case scenario #6: Mum's the word 18

Helping Patients Understand Their Rights 18

Notice of privacy practices 18

Security 19

Security: What you can do 20

Security: What your facility does 20

Personal user IDs and passwords 21

Tips to protect your password 21

Sharing passwords 22

Protecting against computer viruses 23

Unauthorized software 24

Unauthorized hardware 25

Email security 25

Encryption 26
Protecting handheld devices and laptop computers 26
What you can do to protect physical security 27

The Consequences of Breaking the Rules 29

Reporting violations 29
If your facility experiences a breach 30

Obtaining Help 31

In Conclusion 31

Final Exam 33

Answer Key 37

Certificate of Completion 42

ABOUT THE AUTHOR

Kate Borten, CISSP, CISM

Kate Borten, president of The Marblehead Group, offers a unique blend of technical and management expertise, information security and privacy knowledge, and an insider's understanding of the healthcare industry. Her company, founded in 1999, serves the full spectrum of covered entities and their business associates with respect to understanding privacy and security regulations, establishing and enhancing their formal privacy and security programs, and assessing risk and regulatory compliance.

Borten has more than 20 years of experience designing, implementing, and integrating healthcare information systems at world-renowned medical facilities, including Massachusetts General Hospital, where she was responsible for system development. Before founding The Marblehead Group, Borten served as chief information security officer at CareGroup, Inc., where she established a comprehensive information security program that encompassed all entities within its major Boston-area integrated healthcare delivery system. She is an internationally certified information security professional, an Information Systems Security Association (ISSA™) senior member, and a member of the New England chapter's board of directors. She has chaired health sector information security and privacy national conferences and frequently speaks on these topics.

HIPAA Handbook
for Healthcare Staff

Understanding the Privacy and Security Regulations

Intended Audience

This book explains the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules as applicable and relevant to a healthcare organization's general workforce. It also addresses the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 privacy, security, and breach notification provisions, and the 2013 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act (Omnibus Rule).

The intended audience includes:

- Clerical staff, including medical records staff, patient accounting and registration, back office staff, and human resources
- Nutrition services staff
- Nursing assistants

- Housekeeping/facilities staff
- Trainees/students and volunteers
- All other ancillary staff

Learning Objectives

This book explains certain HIPAA and HITECH Act requirements for privacy and security. It addresses workplace practices that protect patient privacy and ensure the security of confidential health information. After reading this book, you should be able to do the following:

- Describe the HIPAA and HITECH Act privacy and security requirements for covered entities
- Define protected health information and explain why protecting patient privacy is important
- Summarize how to protect confidential health information by following proper physical security procedures
- Describe how to protect confidential information you may come across while performing your job
- Contact the correct individual with your questions about protecting patient privacy
- Identify and report suspected privacy and security incidents appropriately

HIPAA Basics

HIPAA is a federal law that protects the privacy of patients and all information about them. HIPAA gives patients the right to have their information kept private and secure. It is more than just a good idea—it is a federal law with penalties (even criminal ones) for violations.

HITECH Act and Omnibus Rule Overview

The American Recovery and Reinvestment Act of 2009 became federal law February 17, 2009. A subset called the HITECH Act enhances and expands the HIPAA Privacy and Security Rules, and adds requirements for breach notification. The HITECH Act not only makes privacy regulations more strict, but it gives more power to federal and state authorities to enforce privacy and security protections for patient data; it also increases the fines for noncompliance. The 2013 Omnibus Rule implements many of the HITECH Act provisions for PHI protection, as well as new protection for genetic information, as mandated by the Genetic Information Nondiscrimination Act (GINA), and new privacy provisions from the U.S. Department of Health and Human Services (HHS). The rule's enforcement date is September 23, 2013.

HIPAA and You

Regardless of your position in the organization, you have constant access to PHI and may regularly communicate with patients and their families and friends, as well as your colleagues. So understanding what HIPAA requires with respect to privacy and security is particularly important for you. No matter where you work in healthcare—a hospital, laboratory,

radiology center, nursing home, or office—you must understand what HIPAA requires of you to keep patient information, in any form (e.g., written, verbal, or electronic), private and secure.

Terms You Should Know

You may hear the following terms mentioned when discussing HIPAA.

Covered entities

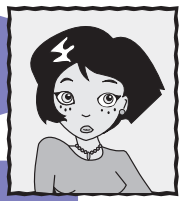
HIPAA's Privacy, Security, Breach Notification, and Omnibus Rules apply to all covered entities (CE). CEs include health plans, healthcare clearinghouses, and most provider organizations, such as physician practices, therapists, dental practices, hospitals, ambulatory facilities, skilled nursing facilities, home health agencies, and pharmacies. Your employer is a CE. All HIPAA covered entities must comply with the HIPAA rules or face civil and even criminal penalties.

Protected health information or PHI

HIPAA establishes rules for when and how patient information may be used and released. Protected health information or PHI includes any information that can be linked to a specific patient, even indirectly. PHI can take any form. It can be electronic, written, or spoken.

PHI includes obvious identifiers such as name, medical record number, or insurance subscriber number. But information without obvious identifiers can still point to one patient. For example, if only one patient underwent a particular procedure this week, the procedure would be enough to identify that patient and would be PHI.

THESE ARE TYPICAL IDENTIFIERS

PHI	Examples
Name	Maria A. Miller
Address	123 Main Street, Millersville, MA 01234
Employer	Millersville Museum of Art
Relatives' names	Thomas Miller, husband
Date of birth	7/21/80
Telephone number	987-654-3210
Email address	iluvhipaa@hotmail.com
Social Security number	123-45-6789
Medical record number	#1123581321
Member or account number	#357111317192329
Fingerprints	
Photographs	
Characteristics (e.g., job) that could identify someone	Museum docent

PHI includes demographic information about the patient, as well as financial and health information if it can be linked to a specific patient. PHI includes billing information, insurance eligibility or coverage, the reason a person is sick or in the hospital, treatments and medications a patient may receive, test results, allergies, observations about a patient's condition, information about past health conditions or treatments, and

discharge planning information. The Omnibus Rule explicitly adds genetic information about individuals and their family members to the definition of PHI.

Minimum necessary/need to know

Only those people with an authorized "need to know" to perform their jobs may have access to PHI. HIPAA requires healthcare workers to use and share or release only the minimum necessary information to perform their jobs without compromising patient care.

Ask yourself several questions before viewing any patient information or disclosing it to someone else:

- Do I need this information to do my job?
- What is the least amount of information I need to perform my job?
- Does the other person need this information to perform his or her job?

Examples of using minimum necessary and need-to-know standards

If you work in food services, you may need to know dietary information about a particular patient to perform your job, but you probably don't need to know other medical information about the patient. Therefore, do not look at other information about this patient or any information about other patients that you don't need to perform your job.

If you are a member of the front office or registration staff, you will encounter PHI as you register patients, deal with insurance matters, and interact with other healthcare providers. But you may access only the parts of the patient medical records that are necessary to perform your job and only the records of the patients you need to access to perform your job. Accessing additional information or information about other patients is a violation of HIPAA.

If you are a member of the housekeeping staff, you might see some discarded test results while you clean a room after a patient has been discharged. Don't look at the information, because you do not need to know the information. And if you recognize a patient's name, you must keep this information to yourself.

Case scenario #1: Celebrity sighting

You walk into a patient's room and are surprised to see the local news station's meteorologist in the hospital bed. During your break in the cafeteria later that day, you ask other staff members if anyone knows why she is in the hospital. The three of you discuss whether her bleached-blonde hair could withstand the recent heavy winds. Your conversation seemed harmless because it was among staff members who all work at your facility. But something tells you it was inappropriate.

Did you do anything wrong?

Yes. The conversation was a HIPAA violation and must be reported to your privacy officer for proper response. You shouldn't have revealed that the meteorologist was a patient. Discussing

her was inappropriate because your coworkers may not have known she was a patient. And your conversation wasn't for job-related purposes; it was just chitchat. Also, the conversation occurred in a very public area—a crowded cafeteria—which is something you should avoid if at all possible. This violated the woman's privacy. You may use, disclose, or tell someone PHI only when it's necessary to perform your job.

Patients' right to privacy has been violated in some well-publicized cases, such as when actor George Clooney received treatment after a motorcycle accident and when former President Bill Clinton underwent cardiac surgery. In both cases, staff members, including physicians, accessed the patient's information, despite their lack of involvement in the patient's care. Disciplinary action resulted in both cases.

TEST YOUR UNDERSTANDING

Which of the following information is permissible to share with a friend?

a. A photograph you took of the newly redecorated waiting room with a few patients present

b. The patient you cared for recently with a highly unusual set of symptoms

c. A completed charity care application

d. Cancer survival rate statistics

Best answer:

d. Discussing a general trend such as cancer survival rates is permissible, but never refer to a specific patient's conditions, diagnosis, or other medical information.

Privacy

Whether they are in a hospital, a physician's office, a laboratory, or another healthcare setting, patients receiving medical care expect privacy. They expect to interact with caregivers away from the public whenever possible, and they expect that caregivers will not share their PHI with individuals who don't need to know it.

Use and release of PHI

HIPAA is not intended to interfere with providing patient care or receiving payment for it. Therefore, HIPAA permits your organization to use and release PHI for several reasons without patient permission. The most common reasons are to provide treatment, obtain payment, and perform certain healthcare operations, such as accreditation and peer review. These activities do not require any patient permission.

In addition to treatment, payment, and healthcare operations, HIPAA permits certain releases of PHI without specific permission from patients for public health and emergency response purposes, as well as when required by law. If releasing patient information is part of your job, ensure that you understand and carefully follow your facility's policy and procedures.

For any other use or disclosure of PHI, your organization first must ask patients, or their legal representatives, for their authorization. With a valid HIPAA authorization form, a patient voluntarily agrees to let your organization use or release information for a particular need.

HIPAA Handbook for Healthcare Staff

Understanding the Privacy and Security Regulations

Kate Borten, CISSP, CISM

This handbook, which provides fundamental privacy and security training for new and seasoned staff, is updated to reflect the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act (also known as the Omnibus Rule). It includes scenarios that depict workplace practices specific to staff and settings to educate them about their role in protecting patient health information. A quiz and certificate of completion help ensure that your staff understands what the law requires.

This is one in a series of HIPAA handbooks for healthcare workers in a variety of roles and settings and business associates to help ensure their compliance with the requirements of the new Omnibus Rule. Other handbooks in the series are tailored for the following members of the healthcare team:

- Behavioral health staff
- Business associates
- Coders, billers, and HIM staff
- Executive, administrative, and corporate staff
- Home health staff
- Long-term care staff
- Nursing and clinical staff
- Nutrition, environmental services, and volunteer staff
- Physicians
- Registration and front office staff

Need to train your entire team or organization?
Volume discounts are available for bulk purchases. Please call 877-233-8828 for more information.

Blend handbook training with our HIPAA Privacy and Security eLearning Library
HCPro's HIPAA eLearning courses are updated to reflect the new provisions set forth in the HIPAA Omnibus Rule. Visit us at *www.hcmarketplace.com,* call 877-233-8828, or email *esales@hcpro.com* for more information on our other training resources.

HHHS2

HCPro
75 Sylvan Street, Suite A-101
Danvers, MA 01923
www.hcmarketplace.com

ISBN: 978-1-61569-228-6
90000
9 781615 692286