

HCP Pro

Omnibus Rule Update

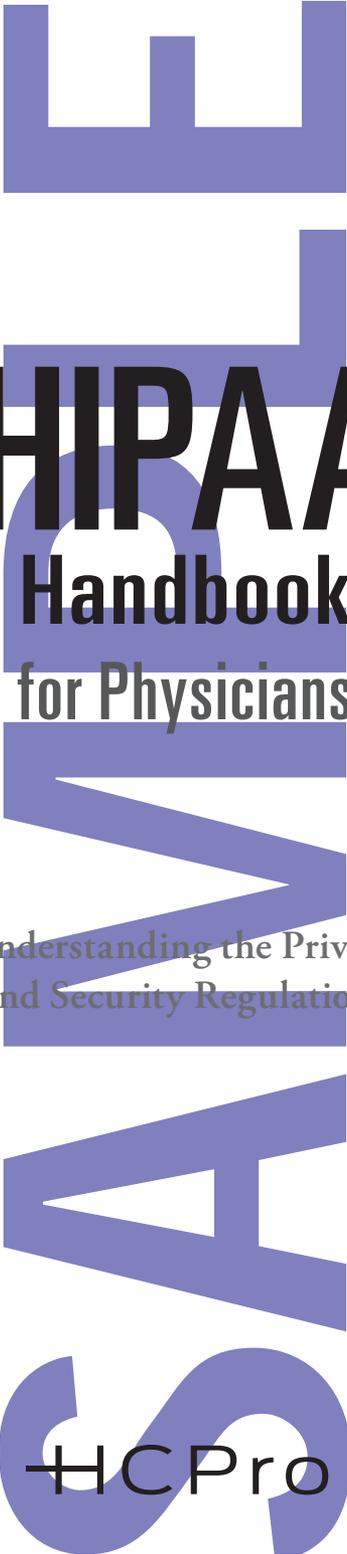
HIPAA

Handbook

for Physicians

**Understanding the Privacy
and Security Regulations**

Kate Borten, CISSP, CISM



HIPAA
Handbook
for Physicians

Understanding the Privacy
and Security Regulations

HCPro

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

Copyright © 2013 HCPro, Inc.

All rights reserved. Printed in the United States of America. 5 4 3 2 1

ISBN: 978-1-61569-243-9

No part of this publication may be reproduced, in any form or by any means, without prior written consent of HCPro, Inc., or the Copyright Clearance Center (978-750-8400). Please notify us immediately if you have received an unauthorized copy.

HCPro, Inc., provides information resources for the healthcare industry. HCPro, Inc., is not affiliated in any way with The Joint Commission, which owns the JCAHO and Joint Commission trademarks.

Kate Borten, CISSP, CISM, Author
Gerianne Spanek, Managing Editor
Mary Stevens, Editor
James T. DeWolf, Publisher and Editorial Director
Mike Mirabello, Production Specialist
Amanda Donaldson, 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
22030

CONTENTS

About the Author	vi
Intended Audience	1
Learning Objectives	2
HIPAA Basics	3
What is HIPAA?.....	3
What are the HITECH Act and the Omnibus Rule?.....	3
HIPAA and you.....	4
Terms You Should Know	4
Covered entities.....	4
Protected health information or PHI.....	5
Business associates.....	5
Need to know/minimum necessary.....	6
Even physicians don't need to know everything.....	7
Case scenario #1: Celebrity sighting.....	7
Privacy	8
Use and Release of PHI	8
Treatment, payment, and healthcare operations.....	8
Other PHI releases not requiring permission.....	8
Family and friends.....	10



HIPAA authorizations.....	11
Case scenario #2: Sometimes you need to vent.....	13
What your facility does to protect confidentiality.....	14
Incidental disclosures.....	15
Avoiding incidental disclosures.....	15
High-risk situations.....	16
HIPAA and minors.....	17
HIPAA and domestic abuse.....	18
HIV, substance abuse, and mental health records.....	18
Psychotherapy notes.....	19
HIPAA and marketing.....	19
HIPAA and fundraising.....	20
Sale of PHI.....	21
HIPAA and research.....	21
Patient Rights.....	23
Notice of privacy practices.....	23
Access to a patient's own PHI.....	24
Amending a medical record or other PHI.....	25
Your role in amending a medical record.....	25
Requests for confidential communication.....	26
Restricting PHI use and disclosure.....	26
Accounting of disclosures.....	27
HIPAA and Security.....	28
Security: What you can do.....	28

Security: What your organization must do 29

Ways to protect physical security 29

Personal user IDs and passwords 30

Case scenario #3: Log on, log off 32

Protecting against computer viruses 33

Unauthorized software 33

Unauthorized hardware 34

Email security 34

Encryption 35

Protecting portable computers and other devices 35

Portable electronic medical devices 36

Remote access 37

The Consequences of Breaking the Rules 37

Reporting violations 38

If your facility experiences a breach 38

Obtaining Help 39

In Conclusion 40

Final Exam 41

Answer Key 46

Certificate of Completion 50

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 this 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 Physicians

Understanding the Privacy and Security Regulations

Intended Audience

This handbook explains the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules as applicable and relevant to physicians. 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 the following:

- Medical staff physicians
- Licensed healthcare practitioners

Learning Objectives

After reading this handbook, you should be able to do the following:

- Describe how the HITECH Act affects covered entities and business associates
- Summarize how to protect patient privacy while providing clinical care
- Explain patient rights in regard to their medical information
- Determine when disclosures of protected health information are acceptable and when they require authorization
- Protect confidential health information by following proper security procedures in the organization and off-site
- Create effective passwords to protect electronic information
- Identify which information commonly encountered by physicians is protected by HIPAA
- Know how to identify and respond to suspected privacy and security violations

HIPAA Basics

What is HIPAA?

HIPAA is a broad 1996 federal law that establishes basic privacy protections to which all patients are entitled. Its original goal was to make it easier for people to move from one health insurance plan to another as they change jobs or become unemployed. The law also requires that common electronic transactions, such as claims, be in a standard format for healthcare organizations and payers.

What are the HITECH Act and the Omnibus Rule?

The American Recovery and Reinvestment Act of 2009 includes a subset called the HITECH Act. The HITECH Act includes provisions for heightened enforcement of HIPAA and stiffer penalties for privacy and security violations. It also expands the HIPAA Privacy and Security Rules to strengthen patient privacy. Examples include the following:

- Increasing HIPAA's patient rights regarding control of their protected health information
- Limiting use of protected health information for marketing purposes
- Mandating breach notification
- Making business associates directly liable for complying with relevant parts of the Security, Privacy, and Breach Notification Rules (while remaining contractually liable to covered entities)

The 2013 Omnibus Rule implements many of the HITECH Act's provisions, as well as additional changes and protections for patient information. The enforcement date is September 23, 2013.

HIPAA and you

Physicians are privy to more confidential health information than perhaps anyone else in the organization. HIPAA calls upon physicians to keep patient information confidential. Many hospitals have amended their medical bylaws to strengthen confidentiality protections.

Physicians should be aware of certain communication habits and change them if necessary to comply with hospital policy and HIPAA's privacy and security regulations.

Terms You Should Know

Covered entities

HIPAA 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. The organization you work for is a CE.

All HIPAA covered entities must comply with these rules or face civil and even criminal penalties.

Protected health information or PHI

HIPAA sets rules for when and how patients' protected health information or PHI may be used and released. PHI includes any information that can be linked to a specific patient. PHI can take any form. It can be electronic, written, or spoken.

PHI may include 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.

PHI includes demographic information about a 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 to the definition of PHI genetic information about individuals and their family members.

Business associates

A business associate (BA) is a person or entity that performs certain functions or activities involving the use or disclosure of PHI on behalf of, or provides services to, a CE. CEs must have BA contracts protecting PHI as specified by HIPAA's Privacy and Security Rules and amended by the Omnibus Rule. The Omnibus Rule requires most CEs to revise

their BA contracts and have them re-signed. Your organization must ensure that BAs sign these contracts before being permitted access to your PHI.

The types of functions or activities that may make a person or entity a BA include, but are not limited to, billing, transcription, collections, information technology (IT) services, document and data disposal, legal services, management, data aggregation, accreditation, e-prescribing gateways, health information organizations, and patient safety organizations.

Need to know/minimum necessary

Only those individuals with an authorized “need to know” to perform their jobs are permitted to have access to PHI. HIPAA requires healthcare workers to access and share or release only the minimum necessary information to perform their jobs.

HIPAA does not require healthcare practitioners to meet the minimum necessary standard for treatment purposes. Treatment was excluded so healthcare practitioners could exchange all necessary information to appropriately treat patients without concern of providing too much information about them. Deciding which information can be exchanged for treatment purposes is determined by the healthcare practitioner’s professional judgment.

However, this does not mean that healthcare practitioners should exchange patients’ full medical records for treatment purposes. For example, if a primary care physician refers a patient to a specialist, it is

likely not appropriate to share the complete medical record with the specialist. Only share that information which is pertinent.

Even physicians don't need to know everything

As a physician, you work with vast quantities of PHI every day. However, remember that PHI is protected, confidential information. Although you may have access to all patient records through your facility's paper files or computer systems, HIPAA requires that you only access records of patients whom you are treating or consulting and only the information about those patients that you need to perform your role.

Case scenario #1: Celebrity sighting

The shortstop for the Chicago Cubs arrives at your facility for an outpatient procedure on his shoulder. He is there for approximately 12 hours.

During a break in the physicians' lounge, you encounter the physician who is treating the patient. Before long, you are chatting about the famous patient and his procedure, which you are delighted to learn was a success. As you are preparing to return to work, you think about the conversation and wonder whether it was inappropriate.



Did you and your colleague do anything wrong?



Yes. You didn't need to know about the procedure or any other details about the patient's status to perform your own work. You shouldn't ask, and your colleague shouldn't volunteer information about this patient.

Because you aren't caring for the patient, you have violated the "need to know" principle. Your interest was the same as anyone's, simply human curiosity, but HIPAA would consider this a privacy violation even though you may think the conversation was harmless.

Privacy

Patients receiving medical care expect privacy whether they are in a hospital, a physician's office, a laboratory, or another setting. They expect to interact with their physicians or caregivers away from the public whenever possible, and they expect that their PHI will not be shared with individuals who don't have a need to know.

Use and Release of PHI

Treatment, payment, and healthcare operations

HIPAA is not intended to interfere with providing patient care or receiving payment for it. Therefore, HIPAA permits physicians to use and release PHI for several reasons without needing patient permission. The most common reason is for healthcare professionals to provide treatment. In addition, obtaining payment and performing certain healthcare operations, such as accreditation and peer review, are also permitted without any special permission.

Other PHI releases not requiring permission

In addition to treatment, payment, and healthcare operations, HIPAA permits certain releases of PHI for public health and emergency response purposes, as well as when required by law.

HIPAA Handbook for Physicians

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
- Healthcare staff
- Home health staff
- Long-term care staff
- Nursing and clinical staff
- Nutrition, environmental services, and volunteer staff
- 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

HCPPro'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.

HCPPro

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

HHMD2

ISBN: 978-1-61569-243-9



9 781615 692439