

HCP Pro

Omnibus Rule Update

HIPAA Handbook

**for Coders, Billers,
and HIM Staff**

**Understanding the Privacy
and Security Regulations**

Kate Borten, CISSP, CISM



HIPAA **Handbook**

for Coders, Billers, and HIM Staff

**Understanding the Privacy
and Security Regulations**

HCP Pro

HIPAA Handbook for Coders, Billers, and HIM Staff: 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: 978-1-61569-234-7

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
22023

CONTENTS

About the Author	vi
Intended Audience	1
Learning Objectives	2
HIPAA Basics	3
HITECH Act and Omnibus Rule overview.....	3
Terms You Should Know	4
Covered entities.....	4
Protected health information or PHI.....	5
Business associates.....	6
Minimum necessary/need to know.....	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
HIPAA authorizations.....	10
Family and friends.....	11
HIPAA and minors.....	11
HIPAA and domestic abuse.....	12

HIV, substance abuse, and mental health records 13

HIPAA and psychotherapy notes 14

Case scenario #2: Sometimes you need to vent 16

What your facility does to protect confidentiality 16

Faxing 17

Case scenario #3: “Hello, Pete’s Plumbing,
how may I help you?” 18

Patient directory 19

Incidental disclosures 19

High-risk situations 21

HIPAA and marketing 22

HIPAA and research 23

Patient Rights 24

Notice of privacy practices 25

Access to a patient’s own medical record 26

Amending a medical record and other PHI 27

Restricting PHI use and disclosure 28

Accounting of disclosures 28

Requests for confidential communication 29

Security 30

Security: What you can do 30

Security: What your facility does 31

Ways to protect physical security 32

Record storage 33

Personal user IDs and passwords	33
Tips to protect your password.....	33
Protecting against computer viruses	34
Unauthorized software and hardware	35
Email security	35
Encryption	36
Protecting handheld devices and laptop computers.....	37
Portable electronic medical devices.....	37
Remote access.....	38
The Consequences of Breaking the Rules.....	39
Reporting violations	39
If your facility experiences a breach.....	40
Obtaining Help	41
In Conclusion.....	41
Final Exam	43
Answer Key.....	48
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.



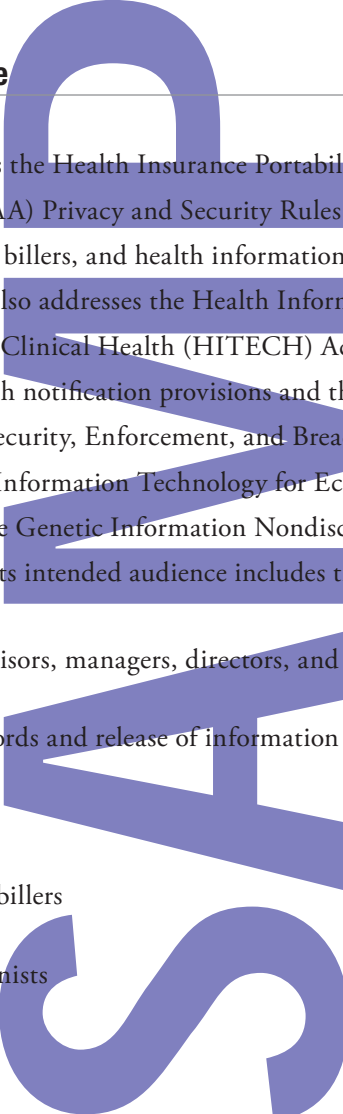
HIPAA Handbook

for Coders, Billers, and HIM 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 coders, billers, and health information management (HIM) staff members. It also addresses the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 privacy, security, and breach notification provisions and 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 (Omnibus Rule). Its intended audience includes the following:

- 
- HIM supervisors, managers, directors, and staff
 - Medical records and release of information staff members
 - File clerks
 - Coders and billers
 - Transcriptionists

Learning Objectives

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

- Describe how these regulations affect covered entities
- Protect patient privacy while performing HIM-related duties, including billing and coding for services provided
- Explain patients' rights for accessing, amending, and updating their medical information
- Follow proper procedures for responding to release of information requests and requests for amendments
- Determine whether disclosures of protected health information are acceptable
- Identify which patient data are permissible to disclose to researchers without patient authorization
- Protect confidential health information by following proper security procedures both in the organization and off-site
- Create effective passwords to protect electronic information
- Know how to identify, report, and respond to suspected privacy and security breaches

HIPAA Basics

HIPAA is a broad federal law that establishes the basic privacy protections to which all patients in the United States are entitled. Its original goal was to make it easier for individuals 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 insurance claims, be in a standard format for healthcare organizations and payers.

Most hospitals and healthcare organizations have always upheld strict privacy and confidentiality policies, but some states had no laws to protect the privacy of **personally identifiable protected health information**. With the enactment of HIPAA, patients' rights to have their health information kept private and secure became more than just an ethical obligation of physicians and hospitals—it became federal law, with civil and even criminal penalties for violations.

As a member of the HIM/medical records staff, you have constant access to protected health information, and you may regularly communicate with patients and their families—and your colleagues. So it's particularly important for you to understand what HIPAA requires with respect to privacy and security.

HITECH Act and Omnibus Rule overview

The American Recovery and Reinvestment Act of 2009 became federal law February 17, 2009. A subset is the HITECH Act, which makes privacy regulations stricter, gives federal and state authorities more power to enforce privacy and security protections for patient data, and

increases civil penalties. The federal government has made transitioning to electronic health records a priority and has increased compliance scrutiny to ensure that the transition does not compromise patient privacy. The HITECH Act expands the HIPAA Privacy Rule and Security Rule to strengthen patient privacy. It increases HIPAA's patients' rights regarding control of their protected health information, limits disclosure of protected health information for marketing purposes, protects it from unauthorized use and disclosure by making business associates directly accountable to the government for parts of the HIPAA rules while remaining contractually liable to healthcare organizations, and mandates breach notification.

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.

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. Your

employer is a CE. All HIPAA covered entities must comply with these HIPAA 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 or health plan member. 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. Typical identifiers include names, addresses, employers, names of relatives, dates of birth, telephone numbers, email addresses, Social Security numbers, medical record numbers, member or account numbers, fingerprints, photographs, and characteristics that can identify an individual, such as an unusual job.

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 it 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 genetic information about individuals and their family members to the definition of PHI.

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. The HITECH Act and Omnibus Rule make BAs directly liable for compliance with the Security Rule and relevant portions of other HIPAA rules.

Even though BAs are now directly liable, CEs must have special contracts with their BAs to protect patient information. HIPAA's Privacy and Security Rules specify the content of BA contracts. The Omnibus Rule changes require most CEs to revise their BA contracts and have them re-signed by September 23, 2013. Your organization must ensure that new BAs sign these contracts before being given access to your PHI.

The types of functions or activities that may make a person or entity a BA include billing, transcription, collections, information technology (IT) services, legal services, management, data aggregation, accreditation, record storage, data and document disposal, e-prescribing gateways, health information organizations, and patient safety organizations.

Minimum necessary/need to know

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

Ask yourself the following questions before accessing patient information:

- Do I need this information to perform my job and provide good patient care?
- What is the least amount of information I need to perform my job?

Case scenario #1: Celebrity sighting

You are transcribing an operative report when you recognize the patient’s name—he’s the Chicago Cubs’ shortstop. Physicians at your facility performed an outpatient procedure on his shoulder. During lunch in the cafeteria later that day, you see your good friend who is a hospital volunteer. You tell her about the celebrity patient and his procedure.



Did you do anything wrong?



Yes. Your friend doesn’t need this information to perform her job, so telling her about the celebrity patient and his procedure was inappropriate. Under HIPAA, this was a privacy violation and must be reported promptly to your supervisor or your privacy officer. 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 accessed the patient's information despite their lack of involvement in his care. Disciplinary action ensued.

Privacy

Patients receiving medical care expect privacy whether they are in a hospital, a physician's office, a laboratory, or another healthcare setting. They expect to interact with their physicians or caregivers away from the public whenever possible, and they expect that their caregivers will not share their PHI 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 healthcare staff members to use and release PHI to perform their jobs for several reasons without needing patient permission. The most common reasons are to provide treatment, obtain payment (e.g., via transcription, coding, and billing), and perform certain healthcare operations (e.g., accreditation and peer review). These activities do not require any patient permission under HIPAA.

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.

Examples of scenarios in which your organization may be subject to laws and regulations permitting or requiring release of PHI include the following:

- Reporting certain communicable diseases and other conditions to state health agencies
- Reporting certain information about medical devices that break or malfunction to the U.S. Food and Drug Administration
- Reporting suspected child abuse or incapacitated elder abuse or neglect to law enforcement officials or your state's human services agency
- Responding to police requests for certain information about patients to determine whether they are suspects in a criminal investigation
- Responding to court orders
- Reporting cases of suspicious deaths or certain suspected crime victims, such as individuals with gunshot wounds or burns that may be due to arson
- Warning those in the community (and law enforcement officials) when a patient has made a credible threat to harm someone
- Providing information in a medical emergency

The Omnibus Rule adds another public health situation not requiring formal authorization. Providers now are permitted to release a student's immunization status to schools when schools are required by law to obtain this information and when there is informal agreement, such as a telephone call from a parent. Providers must limit the disclosure to immunization status **only and must document the agreement** from the parent, guardian, or adult student.

HIPAA authorizations

CEs are permitted to use and release PHI for treatment, payment, and healthcare operations, as well as for public health and other purposes serving the public good without first obtaining an authorization—formal written permission—from patients. The HIPAA Privacy Rule explains other special situations when CEs must give patients an opportunity to agree or disagree with the way their PHI is used or released but that do not require a formal authorization. However, for any other use or disclosure of PHI, CEs first must ask patients, or their legally appointed representatives, for their authorization. With an authorization, the patient voluntarily agrees to let your organization use or release the information for a particular need.

A valid HIPAA authorization form must be completed with a description of the specific PHI to be used or disclosed, the reason or purpose for this use or disclosure, the party to whom the PHI will be released, and an expiration date (e.g., one month from signing) or event (e.g., “upon transmittal”). Your facility's authorization form also must state that signing is voluntary and that the patient may revoke the authorization at any time, although this doesn't undo any action already

undertaken; provide notice that the patient has a right to receive a copy of the authorization; and provide the name of your organization (i.e., the organization releasing the PHI). The patient or the patient's personal representative must sign and date the authorization.

Note: *Providers cannot refuse to treat patients who won't sign authorization forms.*

Ensure that you know your organization's policies before releasing information, and confirm that your situation is approved. When in doubt, consult your supervisor or privacy officer before releasing information that is not authorized by the patient.

Family and friends

HIPAA requires you to obtain permission from a patient before disclosing PHI to family members or friends. If an individual is directly involved in the patient's care or payment for care, then the patient's informal permission is acceptable, but it must be documented in the patient record. In this case, release only the information relevant to care or payment. Obtaining the patient's written authorization is preferable and is required in cases other than releasing information to an individual with a care or payment relationship. Without an authorization, you may release only the information in your facility's patient directory.

HIPAA and minors

HIPAA relies on state laws to define minors and to specify when minors must give permission before a provider can release their PHI to parents or

guardians. Generally, if a minor may consent for treatment in your state, the minor must also sign an authorization to release documentation about that treatment. Generally, providers are not required to disclose information to a parent or guardian in these situations:

- If you believe that the minor has been the victim of domestic violence, abuse, or neglect by the parent or guardian or that disclosures to the personal representative could endanger the minor
- If you decide that it is not in the minor's best interest to treat the parent or guardian as the minor's personal representative
- If the minor is emancipated
- If the minor is seeking treatment for family planning, psychiatric counseling, or substance abuse (substance abuse information is specifically protected by another federal law)

HIPAA and domestic abuse

HIPAA deals with abuse differently depending on whether it is abuse of a child or of an adult, elder, or disabled person. Note that HIPAA is a basic privacy “floor” or minimum standard. Generally, state laws are more specific and stringent than HIPAA with respect to these matters, and you must follow the law that provides the most privacy protection. HIPAA generally gives healthcare providers broader authority to disclose PHI in cases of child abuse than it does for abuse of adults. HIPAA does not limit the information you may disclose in cases of child abuse. However, some laws impose stricter requirements for PHI disclosure for cases involving the abuse of adults.

HIPAA

Handbook

for Coders, Billers, and HIM 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
- Executive, administrative, and corporate staff
- Healthcare 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.

HCPro

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

HHCBH2

ISBN: 978-1-61569-234-7



9 781615 692347