

HCP Pro

***Omnibus Rule Update***

# HIPAA

## Handbook

### for Long-Term Care Staff

**Understanding the Privacy  
and Security Regulations**

**Kate Borten, CISSP, CISM**



**HIPAA**  
**Handbook**  
for Long-Term Care Staff

Understanding the Privacy  
and Security Regulations

HCPro

*HIPAA Handbook for Long-Term Care 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: 978-1-61569-222-4

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](mailto:customerservice@hcpro.com)

Visit HCPro online at: [www.hcpro.com](http://www.hcpro.com) and [www.hcmarketplace.com](http://www.hcmarketplace.com).

05/2013  
22027

# CONTENTS

<b>About the Author</b> .....	<b>vi</b>
<b>Intended Audience</b> .....	<b>1</b>
<b>Learning Objectives</b> .....	<b>2</b>
<b>HIPAA Basics</b> .....	<b>3</b>
<b>HITECH Act and Omnibus Rule Overview</b> .....	<b>4</b>
<b>Terms You Should Know</b> .....	<b>5</b>
Covered entities.....	5
Protected health information or PHI.....	5
Business associates.....	6
Minimum necessary/need to know.....	7
Case scenario #1: We need to talk.....	8
Minimum necessary/need to know: Ask yourself.....	9
<b>Privacy</b> .....	<b>9</b>
Case scenario #2: Start spreading the news.....	10
<b>Use and Release of PHI</b> .....	<b>11</b>
Treatment, payment, and healthcare operations.....	11
Special cases of permitted disclosures.....	11
Disclosure of PHI to residents' family and friends.....	13

HIPAA and minors .....	13
HIV, substance abuse, mental health records, and psychotherapy notes.....	14
HIPAA authorization .....	15
Faxing.....	16
Case scenario #3: Where’s my fax?.....	17
Case scenario #4: You don’t want to be on this list .....	17
What your organization does to protect confidentiality .....	18
Incidental disclosures .....	19
<b>Resident Rights.....</b>	<b>20</b>
Notice of privacy practices.....	20
Access to a resident’s own PHI .....	21
Amending a medical record or other PHI .....	22
Restricting PHI use and disclosure.....	23
Accounting of PHI disclosures .....	23
<b>Security.....</b>	<b>24</b>
Security: What you can do.....	24
Security: What your organization does.....	25
Personal user IDs and passwords .....	26
Tips to protect your password.....	27
Case scenario #5: I need a favor while I’m basking in the sun ....	28
Physical security.....	28
Case scenario #6: I need caffeine .....	29
Destruction of PHI.....	30

Protecting against computer viruses .....	30
Unauthorized software and hardware .....	31
Email security .....	32
Encryption .....	32
Off-site security .....	33
Protecting laptop computers and other portable devices .....	33
Case scenario #7: The absentminded administrator .....	34
Portable computers and viruses.....	35
<b>The Consequences of Breaking the Rules.....</b>	<b>35</b>
Reporting violations .....	36
If your facility experiences a breach .....	37
Breach notification requirements.....	37
<b>Obtaining Help .....</b>	<b>38</b>
<b>In Conclusion.....</b>	<b>39</b>
<b>Final Exam .....</b>	<b>41</b>
<b>Answer Key.....</b>	<b>45</b>
<b>Certificate of Completion.....</b>	<b>50</b>

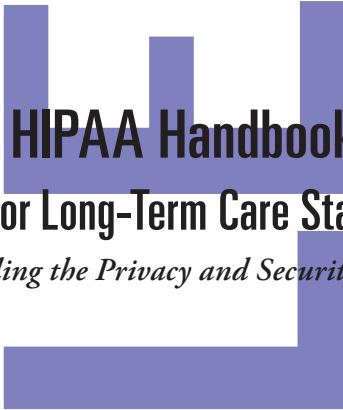
# ABOUT THE AUTHOR

## **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 Long-Term Care 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 long-term care management, staff members, and volunteers. 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:

- Facility owners
- Chief executive officers
- Chief operating officers
- Chief financial officers
- Therapists
- Nursing directors
- Nursing management
- Contracted staff



- Administrators
- Certified nursing assistants
- Department heads
- Housekeeping staff
- Nurses
- Volunteers
- Licensed vocational nurses
- Vendors
- Licensed practical nurses
- Administrative staff
- Minimum data set coordinators
- Students

### Learning Objectives

---

This book explains certain HIPAA and HITECH Act requirements for privacy and security of patient information. It covers 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, security, and breach notification 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 broad federal law that establishes the basic privacy protections to which all U.S. patients 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 form for healthcare organizations and payers. The government has made transitioning to electronic health records a priority and has increased scrutiny to ensure that the transition does not compromise patient privacy.

Most hospitals and healthcare organizations have always had strict privacy and confidentiality policies, but there was no overall federal law protecting the privacy and security of personally identifiable health information.

With the enactment of HIPAA, patients' right to have their health information kept private and secure became more than just an ethical obligation of physicians, hospitals, and other healthcare facilities such as

this one—it became federal law with civil and even criminal penalties for violations.

Whether you are a facility owner, department head, administrator, nurse, therapist, housekeeping staff member, student, volunteer, or vendor, you have access to patient information. You also may regularly communicate with patients, their families and friends, and your colleagues. Understanding what HIPAA requires with respect to privacy and security is especially important.

No matter where you work in healthcare, you must understand what HIPAA requires of you to keep patient information, in any form (e.g., written, oral, or electronic), private and secure.

## **HITECH Act and Omnibus Rule Overview**

---

The American Recovery and Reinvestment Act of 2009 became federal law February 17, 2009. The HITECH Act, a subset of that law, enhances HIPAA's privacy and security regulations. Further, it gives more power to federal and state authorities to enforce privacy and security protections for patient data, and it significantly raised the penalties for noncompliance.

More specifically, the HITECH Act limits use of patient information for marketing purposes, gives patients new rights regarding their information, makes business associates directly liable for compliance (while remaining contractually liable to covered entities), and mandates breach notification to affected patients and the U.S. Department of Health and Human Services (HHS).

The 2013 Omnibus Rule implements many of the HITECH Act's provisions as well as new protection for genetic information, as mandated by the Genetic Information Nondiscrimination Act (GINA), and new privacy provisions from the HHS. The rule strengthens requirements in the Breach Notification Rule, and it clarifies and extends the definition of business associate. The Omnibus Rule's material changes affect most, if not all, covered entities and their business associates, requiring new contracts and new privacy notices. 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 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 can take any form including electronic, paper, and spoken. PHI includes any information that can be linked to a specific patient or resident.

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

PHI includes demographic information about the patient as well as financial and health information. PHI includes, for example, billing information, insurance eligibility or coverage, the reason a person is sick or in the facility, information about past health conditions or treatments, treatments and medications a resident receives, test results, photographs and radiology images, allergies, and observations about a resident's condition. 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 parts of other HIPAA rules.

Even though BAs have become directly liable for certain provisions, CEs must continue to have BA contracts protecting PHI as specified by HIPAA's Privacy and Security Rules and amended by the Omnibus Rule. The Omnibus Rule changes require most CEs to revise their BA contracts and have them re-signed by September 23, 2013. Going

forward, 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, but are not limited to, billing, transcription, collections, information technology (IT) services, document and data storage and disposal, legal services, management, data aggregation, accreditation, e-prescribing gateways, health information organizations, and patient safety organizations.

### ***Minimum necessary/need to know***

HIPAA requires that organizations follow the principle of minimum necessary. Only individuals with an authorized “need to know” to perform their jobs may have access to PHI. And HIPAA requires individuals to access and share only the minimum necessary information to perform their jobs without compromising resident healthcare.

Physicians, nurses, therapists, dietitians, and other caregivers use PHI to determine an individual’s health status and which services are necessary. The billing department uses PHI to bill residents and their insurers for services and items provided. Physicians and quality control directors review PHI to ensure that residents receive good care. These are all examples of treatment, payment, and healthcare operations—all permissible under HIPAA without obtaining resident approval.

All staff members of organizations that provide long-term care contribute to the quality of resident care. However, this doesn’t mean everyone needs to see health information pertaining to all residents.

And it doesn't mean everyone who cares for a particular resident necessarily needs to see all of the information about that resident.

Many employees and other workforce members have no access to resident information, either via computer or on paper, because they don't need to know this information. This is an important phrase to remember—need to know. If you don't need to know confidential resident information to perform your job, you will not be given access to it. This means you should not access or view medical records or other PHI, either on a computer screen or on paper.

You are responsible for safeguarding resident information in your possession. Don't leave it unattended or in areas where others can see it. This is especially important in public buildings, provider locations, and areas with heavy pedestrian traffic.

### ***Case scenario #1: We need to talk***

Two nurses need to discuss a resident's treatment, and they need a place to do so privately.



**Must facilities provide a soundproof room for such conversations?**



Privacy regulations don't require healthcare organizations to provide private or soundproof rooms. However, staff members must take reasonable measures to avoid being overheard. If a private room is not available, discuss residents in an out-of-the-way location, lower your voice, and be discreet.

# HIPAA Handbook for Long-Term Care 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
- Healthcare staff
- Home health 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

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](http://www.hcmarketplace.com), call 877-233-8828, or email [esales@hcpro.com](mailto:esales@hcpro.com) for more information on our other training resources.

HHLTCS2

# HCPPro

75 Sylvan Street, Suite A-101  
Danvers, MA 01923  
[www.hcmarketplace.com](http://www.hcmarketplace.com)

ISBN: 978-1-61569-222-4

