

HCP Pro

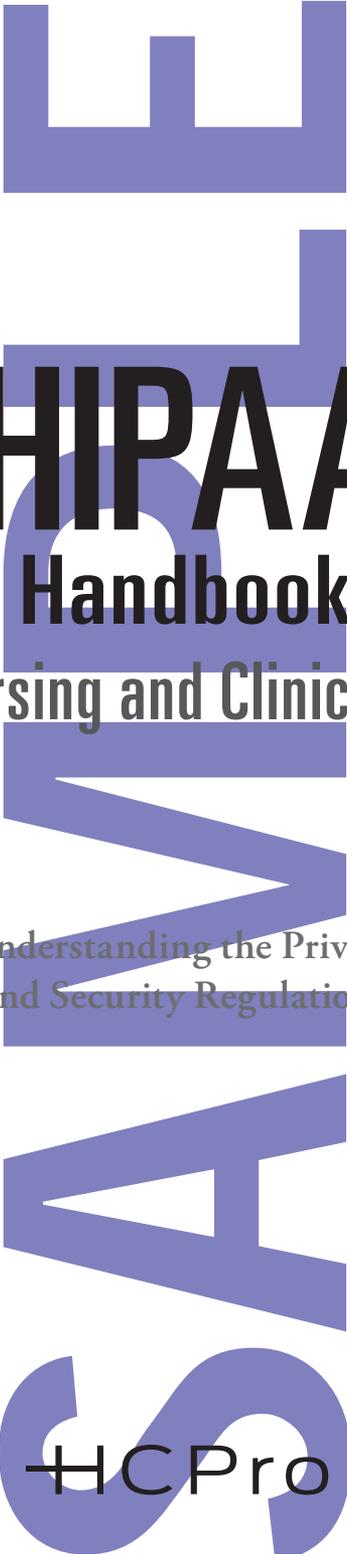
Omnibus Rule Update

HIPAA Handbook

**for Nursing and
Clinical Staff**

**Understanding the Privacy
and Security Regulations**

Kate Borten, CISSP, CISM



HIPAA Handbook

for Nursing and Clinical Staff

Understanding the Privacy
and Security Regulations

HCP Pro

HIPAA Handbook for Nursing and Clinical 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: 978-1-61569-231-6

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
22028

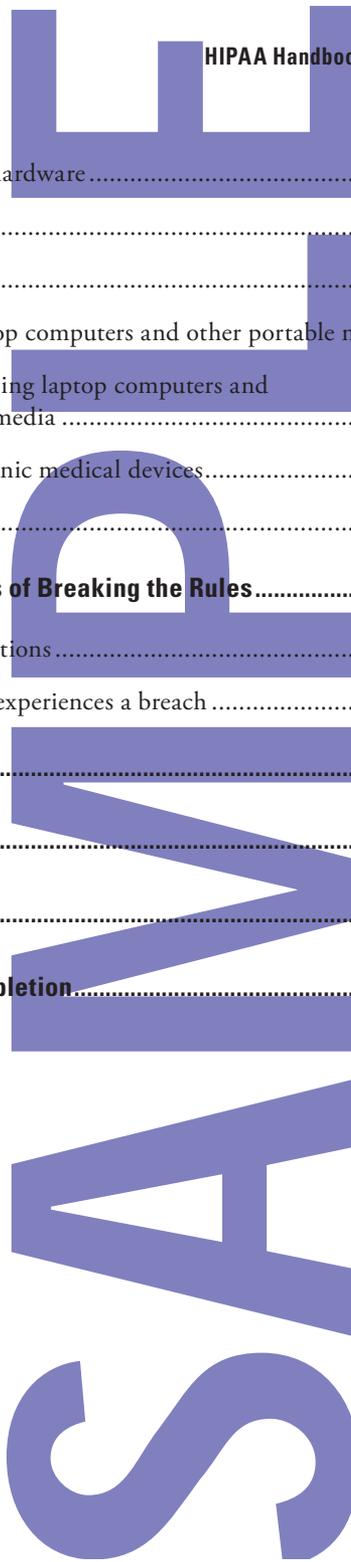
CONTENTS

| | |
|--|-----------|
| About the Author | vi |
| Intended Audience | 1 |
| Learning Objectives | 2 |
| HIPAA Basics | 2 |
| What is HIPAA?..... | 2 |
| What are the HITECH Act and the Omnibus Rule?..... | 3 |
| Terms You Should Know | 4 |
| Covered entities..... | 4 |
| Protected health information or PHI..... | 4 |
| Business associates..... | 6 |
| Minimum necessary/need to know..... | 6 |
| 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..... | 9 |
| Family and friends..... | 10 |
| HIPAA and minors..... | 11 |
| HIPAA and domestic abuse..... | 12 |

HIPAA Handbook for Nursing and Clinical Staff

| | |
|--|-----------|
| HIPAA authorization | 13 |
| Case scenario #2: Sometimes you need to vent | 14 |
| What your facility does to protect confidentiality | 16 |
| Faxing | 16 |
| Case scenario #3: “Hello, Pete’s Plumbing, how may I help you?” | 17 |
| Patient directory | 18 |
| Incidental disclosures | 19 |
| Avoiding incidental disclosures | 19 |
| High-risk situations | 20 |
| Patient Rights | 21 |
| Notice of privacy practices | 21 |
| Access to a patient’s own medical record and other PHI | 22 |
| Amending a medical record and other PHI | 23 |
| Restricting PHI use and disclosure | 24 |
| Requests for confidential communication | 24 |
| Requesting an accounting of PHI disclosures | 25 |
| HIPAA and Security | 26 |
| Security: What you can do | 26 |
| Security: What your organization must do | 27 |
| Ensuring physical security | 27 |
| Personal IDs and passwords | 28 |
| Sharing passwords | 29 |
| Unauthorized software | 30 |

| | |
|---|-----------|
| Unauthorized hardware | 30 |
| Email security | 30 |
| Encryption | 31 |
| Protecting laptop computers and other portable media | 31 |
| Tips for protecting laptop computers and other portable media | 32 |
| Portable electronic medical devices | 32 |
| Remote access | 33 |
| The Consequences of Breaking the Rules | 33 |
| Reporting violations | 34 |
| If your facility experiences a breach | 34 |
| In Conclusion | 35 |
| Final Exam | 37 |
| Answer Key | 41 |
| Certificate of Completion | 42 |

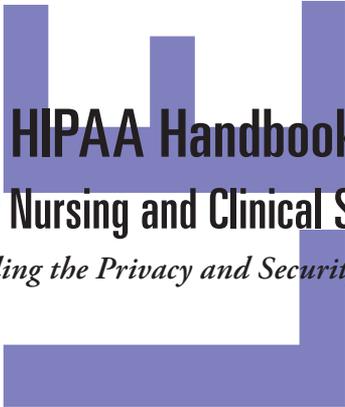


ABOUT THE AUTHOR

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 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 Nursing and Clinical Staff

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 nursing and clinical staffs. It also addresses the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act 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).

Its intended audience includes:

- Nurses
- Nurse practitioners
- Physical therapists
- Respiratory therapists
- Medical assistants
- Licensed vocational nurses
- Technicians
- Speech-language pathologists

Learning Objectives

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

- Describe how HIPAA and the HITECH Act affect covered entities
- Summarize how to protect patient privacy without compromising clinical care
- Explain patient rights regarding their medical information
- Determine whether disclosures of protected health information are acceptable
- Protect confidential health information by following proper security procedures both in the organization and off-site
- Create effective passwords to protect electronic information
- Identify which information commonly encountered by nurses or clinical staff members is protected by HIPAA
- Identify and report privacy and security violations

HIPAA Basics

What is HIPAA?

HIPAA is a broad federal law that establishes the 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?

In February 2009, President Barack Obama signed the American Recovery and Reinvestment Act of 2009 into law. A subset, the HITECH Act, enhances and expands HIPAA's privacy and security protections and adds new provisions.

The HITECH Act includes provisions for heightened enforcement of HIPAA and stiffer penalties for HIPAA violations. It expands the HIPAA Privacy Rule to strengthen patient privacy by increasing HIPAA's patient rights regarding control of protected health information and limiting use of protected health information for marketing purposes. The Act mandates breach notification to affected patients and the U.S. Department of Health and Human Services (HHS). And it extends requirements to business associates.

The 2013 Omnibus Rule implements many of the HITECH Act provisions pertaining to protected health information, as well as new protection for genetic information, as mandated by the Genetic Information Nondiscrimination Act (GINA), and new privacy provisions from HHS. The rule's enforcement date is September 23, 2013.

Terms You Should Know

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, hospitals, ambulatory facilities, skilled nursing facilities, and home health agencies. The organization you work for 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.

However, 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.

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 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 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. Your organization must ensure that new 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.

Minimum necessary/need to know

Only those individuals with an authorized "need to know" to do their jobs are permitted to have access to PHI. HIPAA requires healthcare workers to have access to and disclose only the minimum necessary information to do their jobs.

It's helpful to ask yourself the following questions before accessing any patient information:

- Do I need this to do my job and provide good patient care?
- What is the least amount of information I need to do my job?
- If I am sharing patient information with someone else, does the other person need this information to perform his or her job?

All members of the hospital workforce contribute to the quality of care. But this doesn't mean everyone needs to see health information about patients. And it doesn't mean everyone who cares for patients should see information about all patients. You are permitted to access only the records of patients with whom you are working.

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.

A fellow staff member calls you over to her desk. "Check it out!" she whispers. "He lives right near you!" You realize she's accessed the player's medical record. Then you notice that another nurse nearby has done the same thing to learn the player's diagnosis and estimate how long he'll be out of the lineup—his fantasy baseball team depends on it.

You recently underwent extensive training that addresses HIPAA's patient confidentiality requirements, and your colleagues' actions concern you.



What should you do?



This is a HIPAA violation that must be reported. Promptly contact your manager or your organization's privacy official. It is your responsibility to protect the patient's privacy by reporting these violations, and your organization may not retaliate against you.

Most likely, your organization's audit trails flag unacceptable access to patient records. The offending employees may be warned, reprimanded, or suspended for viewing and sharing the record because they weren't doing so for a job-related purpose.

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 healthcare staff members to use and release PHI to perform their job for several reasons without needing 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.

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 and when required by law.

Examples of scenarios in which your organization may be subject to laws 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

HIPAA

Handbook

for Nursing and Clinical 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
- Long-term care 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

HPro'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.

HPro

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

HHNCS2

ISBN: 978-1-61569-231-6



9 781615 692316