

HCP Pro

Omnibus Rule Update

HIPAA Handbook

**for Registration and
Front Office Staff**

**Understanding the Privacy
and Security Regulations**

Kate Borten, CISSP, CISM



HIPAA

Handbook

for Registration and
Front Office Staff

Understanding the Privacy
and Security Regulations

HCP Pro

HIPAA Handbook for Registration and Front Office 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: 978-1-61569-246-0

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
22031

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..... | 4 |
| Minimum necessary/need to know..... | 5 |
| Minimum necessary/need to know: Ask yourself..... | 6 |
| Case scenario #1: Celebrity sighting..... | 7 |
| Privacy | 7 |
| Case scenario #2: Sometimes you need to vent..... | 9 |
| What your facility does to protect confidentiality..... | 10 |
| Faxing..... | 11 |
| Case scenario #3: Joe the plumber..... | 12 |
| Use and Release of PHI | 12 |
| Treatment, payment, and healthcare operations..... | 12 |
| Other PHI releases not requiring permission..... | 13 |

HIPAA Handbook for Registration and Front Office Staff

| | |
|---|-----------|
| HIPAA authorizations..... | 14 |
| Family and friends..... | 15 |
| HIPAA and minors..... | 16 |
| HIV, substance abuse, and mental health records..... | 17 |
| Psychotherapy notes..... | 17 |
| Patient directory..... | 17 |
| Opting out of the patient directory..... | 18 |
| Visiting clergy..... | 19 |
| Incidental disclosures..... | 19 |
| Minimize incidental disclosures..... | 20 |
| High-risk situations..... | 20 |
| Patient Rights..... | 22 |
| Notice of privacy practices..... | 22 |
| Access to a patient’s own medical record and other PHI..... | 24 |
| Amending a medical record and other PHI..... | 25 |
| Requests for confidential communication..... | 26 |
| Restricting PHI use and disclosure..... | 26 |
| Accounting of PHI disclosures..... | 27 |
| Security..... | 28 |
| Security: What you can do..... | 28 |
| Security: What your facility does..... | 29 |
| Keep your physical space secure..... | 30 |
| Personal user IDs and passwords..... | 30 |
| Tips to protect your password..... | 31 |

Protecting against computer viruses 32

Unauthorized software and hardware 32

Email security 33

Encryption 34

Tips for protecting handheld devices and laptop computers..... 34

The Consequences of Breaking the Rules 35

 Reporting violations 36

 If your facility experiences a breach 36

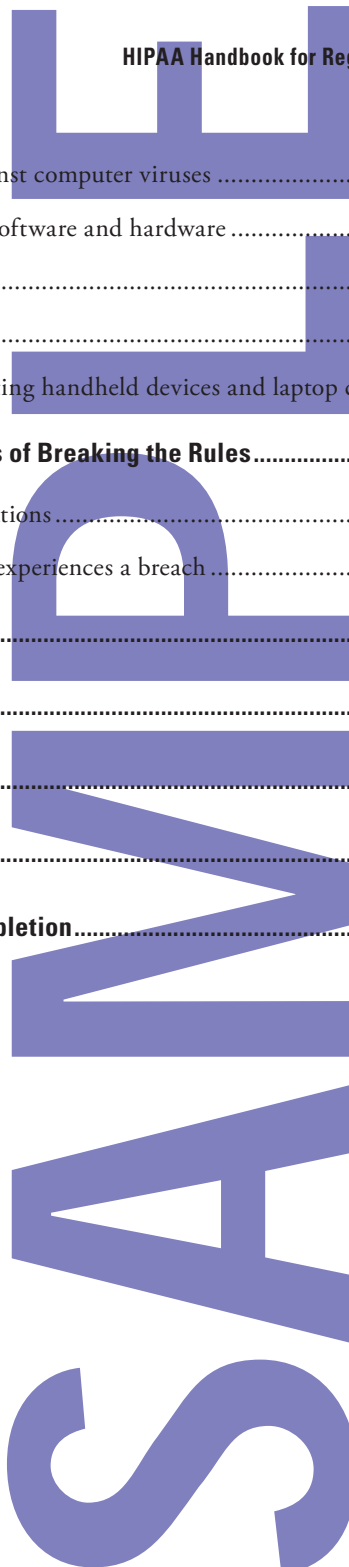
Obtaining Help 37

In Conclusion..... 38

Final Exam 39

Answer Key..... 45

Certificate of Completion..... 50

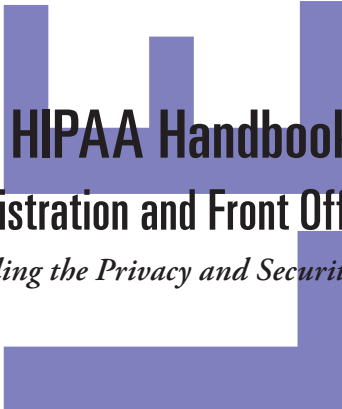


ABOUT THE AUTHOR

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 Registration and Front Office 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 registration 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 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:

- Registration staff
- Front desk staff
- Patient access staff

Learning Objectives

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

- Describe how HIPAA and the HITECH Act affect covered entities and you
- Summarize how to protect patient privacy and confidentiality during the registration process
- Explain patients' rights with respect to accessing their medical information
- Follow proper procedures for giving new patients your facility's notice of privacy practices
- Determine whether disclosures of protected health information are acceptable
- Protect confidential health information during the registration process by following proper security procedures
- Create effective passwords to protect electronic information
- Identify which information commonly encountered by registration or patient access staff members is protected by HIPAA

HIPAA Basics

HIPAA is a broad federal law that establishes basic privacy protections to which all U.S. patients are entitled. It also establishes obligations for organizations such as this one to follow.

Most hospitals and healthcare organizations have always had strict privacy and confidentiality policies, but until HIPAA there was no federal law to protect the privacy of personally identifiable health information. Under HIPAA, patients' right 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.

Whether you are a member of the registration staff, a member of the patient access staff, or in a similar position, you have constant access to PHI and may regularly communicate with patients and their families and friends, as well as your colleagues. 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, skilled nursing facility, 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.

HITECH Act and Omnibus Rule overview

The American Recovery and Reinvestment Act of 2009 includes a subset called the HITECH Act. Its goals include expanding HIPAA's privacy protections and requiring patient notification when there is a breach.

The HITECH Act also gives federal and state authorities more power to enforce privacy and security protections for patient data, and it raises the fines for noncompliance.

The 2013 Omnibus Rule implements many of the HITECH Act's provisions, and adds further privacy protections.

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, dental practices, hospitals, ambulatory facilities, skilled nursing facilities, home health agencies, and pharmacies.

Your employer is a CE. All HIPAA covered entities, including your employer, must comply with all HIPAA rules or face civil and even criminal penalties.

Protected health information or PHI

HIPAA establishes 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.

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

Minimum necessary/need to know

Only individuals with an authorized "need to know" to perform their jobs may have access to PHI. HIPAA requires healthcare workers, including registration and front desk staff, to use and share only the minimum necessary information to perform their jobs.

All members of the workforce at a hospital or other patient care facility contribute to the quality of care. But this doesn't mean everyone needs

to see health information pertaining to all patients. And it doesn't mean everyone who cares for a particular patient must see all of the information about that patient. This means you may not look for an acquaintance's telephone number, check a family member's laboratory results, view a friend's diagnosis via the computer or in the paper record, or access or view the medical record of a celebrity being treated at your facility.

As a registration staff member, you work with vast quantities of PHI every day. Remember that PHI is protected, confidential information. Although you may have extensive access to PHI via your facility's computer systems and paper records, HIPAA requires that you access only the patient information that you need to perform your job. For example, you will see PHI as you register patients, deal with insurance matters, and interact with other healthcare providers. However, you may access only the portions of 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 other patients' information is a violation of HIPAA.

Minimum necessary/need to know: Ask yourself

Ask yourself the following questions before accessing any patient information or disclosing it to someone else:

- Do I need this to perform my job?
- What is the least amount of information I need to perform my job?

- Does the person with whom I'm speaking need to know this information to perform his or her job?

Case scenario #1: Celebrity sighting

You overhear another member of your hospital's registration staff register the mayor of your small town. Later, during lunch in the cafeteria, you inquire about the procedures the mayor is undergoing, and your colleague answers in great detail.



Did you do anything wrong?



Yes. You both violated HIPAA. You shouldn't have asked and your colleague shouldn't have provided this information, because you didn't need it to perform your job. Also, a crowded cafeteria where others could easily overhear you was an inappropriate place for this inappropriate conversation. The patient's right to privacy has been violated in some well-publicized cases. UCLA Medical Center terminated 13 employees and suspended six others in 2008 for inappropriately accessing or viewing singer Britney Spears' medical record.

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, caregivers, and support staff, including registration and front desk staff, 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.

DOS AND DON'TS FOR PROTECTING PRIVACY

| Dos | Don'ts |
|---|--|
| <p>Avoid discussions about patients in elevators, cafeteria lines, nurses' stations, and other public places, both inside and outside the facility</p> | <p>Don't discuss patients other than when necessary for work-related purposes.</p> |
| <p>Keep paper on desks facedown or inside folders when others may pass by. You may have copies of insurance cards, orders, or other documents that contain PHI at your desk. Keep all paperwork facedown or cover it if you walk away, even if only for a moment.</p> | <p>Don't leave appointment schedules, medical records, encounter forms, laboratory requisitions, or other patient documents unattended.</p> |
| <p>Take extra precautions if your child or other guests accompany you to work to ensure that they don't see PHI.</p> | <p>Don't share information that you overhear or see as you work with anyone who doesn't need to know.</p> |
| <p>Discard patient information by shredding it or storing it in a locked container for future cross-shredding and destruction in accordance with organization policy.</p> | <p>Don't forget about reminders to yourself on Post-it® notes or telephone message notepads—they may contain PHI. Paperwork that contains PHI isn't always a formal document.</p> |
| <p>Double-check your mailings and appointment reminders. If you inadvertently address a reminder to the wrong patient, you inappropriately disclose another patient's information, a privacy violation that must be reported to your supervisor or privacy officer for investigation.</p> | <p>Don't forget who is nearby. Registration areas often are in open, crowded locations. Remember that you may not be able to see everyone around you. You could be unaware that someone in a nearby admitting booth who is not visible to you can overhear what you say. Keep your voice as low as possible.</p> |

DOS AND DON'TS FOR PROTECTING PRIVACY (CONT.)

| Dos | Don'ts |
|---|---|
| <p>Be aware of paperwork strewn about when you register a patient at your desk. Turn papers facedown if appropriate to do so. Eyes wander, and the number of individuals who can read upside-down is surprising.</p> | <p>Don't post items containing PHI in public areas. Even patients' thank-you notes, if posted publicly, can be problematic for you if the persons who sent them don't want their visits to your facility made public.</p> |
| <p>Ask patients to step back from the registration area while they wait their turn so they don't overhear information pertaining to others. Keep your voice low and turn away from the public area. Use discretion with respect to saying patients' names or discussing their symptoms. When possible, take patients needing more privacy to a separate area.</p> | <p>Don't leave messages about patient conditions or test results on answering machines or with anyone other than the patient without written permission to do so.</p> |
| <p>Be as discreet as possible. Some organizations assign patient numbers instead of calling them by name, for example. When verifying a patient's date of birth, consider omitting the year. And be extremely careful when discussing the reason for a patient's visit.</p> | <p>Don't leave patient information on printers, fax machines, or otherwise strewn about after you are done reviewing or using it.</p> |

Case scenario #2: Sometimes you need to vent

During breakfast at a local pancake house after a long overnight shift in the emergency department, you and a colleague begin to vent. Your conversation includes a detailed discussion of last night's trauma patients

who were involved in a motor vehicle accident with an allegedly intoxicated driver.



Did you do anything wrong?



Yes. A privacy breach may have occurred if others were listening to your conversation and if you shared sufficient details about any of the patients. This is especially true if an article about the accident appears in your local newspaper or if the accident is the subject of a report on a local television station.

What your facility does to protect confidentiality

Your facility protects confidentiality by doing the following:

- Locking records securely and allowing access only to individuals who need them for their healthcare-related work
- Requiring employees and others with access to electronic patient records to log off their computers when away from their desks
- Turning computer screens away from public view or using privacy filters so that information is not seen accidentally
- Monitoring access to electronic records by maintaining and reviewing audit trails to ensure that the records are being used appropriately
- Cross-shredding any paper that includes PHI before discarding it, or employing a confidential destruction company

HIPAA Handbook

for Registration and Front Office 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
- Nursing and clinical staff
- Nutrition, environmental services, and volunteer staff
- Physicians

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.

HHRFOS2

HCPPro

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

ISBN: 978-1-61569-246-0



9 781615 692460