HCPro

Omnibus Rule Update

HIPAA Handbook

for Nutrition, Environmental Services, and Volunteer Staff

Understanding the Privacy and Security Regulations

Kate Borten, CISSP, CISM

HIPAA Handbook

for Nutrition, Environmental Services, and Volunteer Staff

Understanding the Privacy
and Security Regulations

HCPro

HIPAA Handbook for Nutrition, Environmental Services, and Volunteer Staff: Understanding the Privacy and Security Regulations is published by HCPro, Inc.

ISBN: 978-1-61569-240-8

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
22029

CONTENTS

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 Nutrition, Environmental Services, and Volunteer 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 nutrition and environmental services staff members and volunteers. It also addresses the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 privacy and security 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:

- Nutrition services staff members
- Custodial and janitorial staff members
- Engineers and maintenance staff members
- Volunteers

Learning Objectives

This handbook explains certain HIPAA and HITECH Act requirements for privacy and security. It addresses workplace practices that protect patient privacy and ensure the security of confidential health information. After reading this handbook, you should be able to do the following:

- Describe the HIPAA and HITECH Act privacy and security requirements for covered entities as they pertain to you
- 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 encounter while performing your job
- Contact the correct individual with your questions about protecting patient privacy and reporting privacy and security issues

HIPAA Basics

What is HIPAA?

HIPAA is a federal law that protects the privacy of patients and all information about them. HIPAA gives patients the right to have their information kept private and secure. It is more than just a good idea—it is a federal law with penalties (even criminal ones) for violations.

HITECH Act and Omnibus Rule overview

The American Recovery and Reinvestment Act of 2009 became federal law February 17, 2009. A subset of that law is the HITECH Act, which enhances and expands the HIPAA privacy protections. The HITECH Act makes privacy regulations stricter. It also gives more power to federal and state authorities to enforce privacy and security protections for patient data, it raises the fines for noncompliance, and it requires that patients and the U.S. Department of Health and Human Services (HHS) be notified of breaches. The Omnibus Rule enforces many of the HITECH Act requirements and adds further privacy protections. Your organization is required to comply with all HIPAA rules.

Terms You Should Know

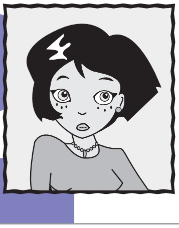
Protected health information or PHI

HIPAA protects all patient information. Protected health information is known as PHI. HIPAA establishes rules for when and how healthcare staff members may use or release patients' PHI.

PHI includes any information that can be linked to a specific patient, even indirectly. It includes demographic information (e.g., person's name), financial information (e.g., insurance numbers), billing information, and health information (e.g., diagnosis codes). PHI can take any form, including paper, electronic, and spoken.

PHI includes obvious identifiers such as name, medical record number, and insurance subscriber number.

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

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 medical information. PHI also includes medical or healthcare-related information if it can be linked to one specific patient, including the following:

- The reason a person is sick or in the hospital
- The treatments and medications a patient may receive
- Test results
- Observations about a patient's condition
- Information about past health conditions or treatments
- Discharge planning information
- Billing information
- Genetic information about a patient and family members

Minimum necessary/need to know

Only staff members who "need to know" PHI to perform their jobs may have access to it. HIPAA requires healthcare workers to use or share only the "minimum necessary" information to perform their jobs. Ask yourself the following questions before viewing and sharing any patient information:

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

- Does the person I am sharing this information with have a work-related need to know it?

You may need to know dietary information about a particular patient to perform your job, but you probably don't need to know other medical information about the patient to perform your job. Therefore, do not look at other information about this patient or any information about other patients. Or perhaps you encounter discarded test results while you clean a room after a patient has been discharged. Don't look at the information, because you do not need to know the information. If you recognize a patient's name, you must keep this information to yourself.

Case scenario #1: Celebrity sighting

You walk into a patient's room and are surprised to see the local television station's meteorologist in the hospital bed. During your break in the cafeteria later that day, you ask other staff members if anyone knows why she is in the hospital. Two other staff members hear your conversation. The three of you discuss whether her bleached-blonde hair could withstand the recent heavy winds. Your conversation seemed harmless because it was among staff members who all work at your facility. But something tells you it was inappropriate.

Q **Did you do anything wrong?**

A Yes. This is a HIPAA violation and must be reported to your privacy officer. You shouldn't have revealed that the meteorologist was a patient. Discussing her was inappropriate because your coworkers may not have known she was a patient. Furthermore, your conversation wasn't for job-related purposes; it was simply chitchat. Also, the conversation occurred in a very public area—a crowded cafeteria—something you should avoid if at all possible. This violated the patient's privacy.

You may use or tell someone PHI only when it's necessary to perform your job. Otherwise, it is generally prohibited. 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, including physicians, accessed the patient's information, despite their lack of involvement in the patient's care. Disciplinary action resulted in both cases.

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 caregivers away from the public whenever possible. They expect that caregivers will not share their PHI with individuals who don't need to know it. Use the following tips to help protect patients' privacy:

- Avoid discussions about patients in elevators and cafeteria lines, at nurses' stations, and other public places, both inside and outside the hospital.
- Return paper patient information to its appropriate location or properly destroy it when you are done using it.

- Be aware of HIPAA's privacy regulations if your children or other guests accompany you to work. Your guests should not be able to see PHI in any form.

- Don't discuss patients with anyone except when necessary for work-related purposes.

- Don't share information that you inadvertently overhear or see with individuals who don't need the information to perform their jobs.

- Don't discuss a patient's condition or treatment with their family members or other visitors. Instead, politely refer these individuals to the clinical staff member who can respond to their questions appropriately.

Discarded patient information

Don't discard patient information in a trash receptacle without shredding it or following your organization's procedures for destroying confidential information. The receptacle could tip over or the contents could fall off a recycling truck and blow down the street. If you see PHI in a trash receptacle, retrieve it and notify your supervisor to ensure its proper disposal.

Case scenario #2: Sometimes you need to vent

You deliver lunch to a patient whom you recognize as a longtime friend of your mother. You chat with her briefly and then return to work. You are careful not to inquire about the reason for her hospitalization. Later that evening, you call your mother to tell her that you saw her friend.

Q **Did you do anything wrong?**

A Yes. You may not tell your family about patients in your facility. Chatting with the patient is permissible, as long as she initiates the conversation. However, you absolutely should not tell your mother that you saw her friend. Sharing information you learn at work with individuals outside of the hospital is a HIPAA violation. This patient may not want others to know she is hospitalized. Telling your mother that you saw the patient violates her friend's privacy. You should not share patient information with anyone who doesn't need to know it. This includes your family and friends.

Patient directory

A patient directory is a list of patients within a facility. It provides limited information to individuals who inquire about a patient by name. HIPAA permits directories to include patients' names, location, and general condition. Patients who desire may be excluded from the directory. If visitors request information about a patient, direct them to the information desk for assistance.

Incidental disclosures

Sometimes you may have incidental access to confidential information. For example, you may overhear a physician speaking to a patient about her diagnosis, or you may hear therapists discussing a patient's treatment plan. This is PHI that must remain confidential, so you should not share this information with anyone else.

Patients' family and friends

HIPAA requires hospitals and other healthcare providers to obtain permission from patients before sharing PHI with their family members or friends. Be careful not to provide patients' families and friends with any information you may have learned while performing your job. If patients, their families, or friends ask you to do so, alert a nurse or other staff member involved in the patient's care so that this individual can assist them.

Responding to patient requests

When patients ask you for a copy of their medical record or request that you update their contact information, speak to a nurse or other staff member who is caring for them. They can assist patients with these requests.

High-risk situations: Elevators, lobbies, and other public places

High-risk areas where you might be tempted to discuss a patient, probably without realizing the risks associated with doing so, include elevators, lobbies, and other public places. Remember that these are places and situations where discussion of patients is inappropriate. Elevators might seem to be a convenient place to converse as you go from floor to floor, but it is probably impossible for other passengers to avoid eavesdropping. Avoid discussing patients in lobbies and other public places, such as cafeterias; keep your voice low or move to a private place if at all possible. And remember to discuss patients only when a work-related need requires you to do so.

HIPAA Handbook

for Nutrition, Environmental Services, and Volunteer 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
- Physicians
- Registration and front office staff

HHNES2

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

ISBN: 978-1-61569-240-8
90000
9 781615 692408