HCPro

Omnibus Rule Update

HIPAA Handbook for Home Health Staff

Understanding the Privacy and Security Regulations

Kate Borten, CISSP, CISM

HIPAA Handbook for Home Health Staff

Understanding the Privacy and Security Regulations

HCPro

HIPAA Handbook for Home Health Staff: Understanding the Privacy and Security Regulations is published by HCPro, Inc.

ISBN: 978-1-61569-237-8

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
22026

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 Home Health 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 home health 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:

- Nurses
- Home health aides
- Therapists
- Agency clerical and billing staff

- Management and human resources employees
- Volunteers

Learning Objectives

This book 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 book, you should be able to do the following:

- Describe the HIPAA, HITECH Act, and Omnibus Rule privacy, security, and breach notification 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 come across while performing your job
- Contact the correct individual with your questions about protecting patient privacy
- Be prepared to identify and report privacy and security violations

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.

Most hospitals and healthcare organizations have always had strict privacy and confidentiality policies, but until HIPAA there was no broad 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, hospitals, home health, and other healthcare organizations—it became federal law, with civil and even criminal penalties for violations.

Whether you are a nurse, home health aide, therapist, volunteer, or a member of your organization's clerical, billing, human resources, or management staff, you have access to protected health information, and you 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, and 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 enhancing and expanding HIPAA's privacy and security protections.

The HITECH Act not only makes privacy regulations more strict but it gives more power to federal and state authorities to enforce privacy and security protections for patient data and it raises the fines for noncompliance. The government has made transitioning to electronic health records (EHR) a priority and has increased privacy scrutiny to ensure that the transition does not compromise patient privacy.

The HITECH Act expands HIPAA's Privacy and Security Rules to strengthen patient privacy by increasing patient rights regarding control over their protected health information, limiting use of protected health information for marketing purposes, and mandating breach notification to affected patients.

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 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'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 must comply with these rules or face civil and even criminal penalties.

Protected health information or PHI

HIPAA includes rules that govern when and how patients' protected health information or PHI may be used and released. PHI can take any form. It can be electronic, written, or spoken. PHI includes any information that can be linked to a specific patient.

Sometimes the information contains a direct identifier that makes the patient's identity obvious, such as name, address, employer, relatives' names, date of birth, telephone number, email address, Social Security number, medical record number, member or account number, fingerprints, photograph, or job title.

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 (e.g., person's name), financial information (e.g., insurance number), billing information, and health information (e.g., diagnosis code).

PHI includes medical or healthcare-related information associated with a patient, including the following, if the patient's identity can be determined from it or other related data:

- Reason a person is sick or receiving home health care
- Treatments and medications he or she may receive
- Test results
- Allergies
- Observations about the patient's condition
- Information about past health conditions or treatments
- Hospital discharge planning information
- Billing information
- Genetic information about the person or family members

Minimum necessary/need to know

Healthcare organizations collect PHI so they can take care of their patients and perform other related functions. However, organizations and their staff may use it only in limited ways. Physicians, nurses,

therapists, dietitians, and other caregivers use patient information to determine which services are necessary. The billing department uses confidential information to bill patients and their insurers for services provided. Physicians and quality control directors review confidential information to ensure that patients receive good care.

All staff members of organizations that provide home health services contribute to the quality of patient care. But that 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 necessarily needs to see all of the information about that patient.

Many employees have no access to patient information, either via computer or on paper, because they don't need to know this information for their job. This is an important phrase to remember—need to know. If you don't need to know patient information to perform your job, you should not access it. Even if you are given access to a records room or electronic patient records, you are permitted to access only the records of patients you are treating or for which you have another work-related need. This means you should not access medical records, either on a computer monitor or on paper, unless it's part of your job.

Minimum necessary/need to know: Ask yourself

Only individuals with an authorized "need to know" to perform their jobs are permitted to have access to PHI. And HIPAA requires health-care workers to use or share only the "minimum necessary" information to perform their jobs. 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: Start spreading the news

A home health worker notices that a coworker's patient is a fellow parishioner. The home health worker accesses the patient's record to learn more and then calls other parishioners to tell them about the patient's condition. Congregation members form a prayer chain and suddenly several hundred individuals know of their fellow parishioner's illness.

Is this disclosure acceptable?

No. This is a HIPAA violation and likely a breach. It must be reported to your supervisor or privacy officer for proper handling. Accessing or viewing patient records for any nonbusiness reason, even if it's with the best intentions, is cause for dismissal, and there are potential legal consequences. Even if you access or view records for a legitimate business reason but then you share this information with others who don't need to know it, you are violating the law and your organization's privacy policy. You are permitted to access patient records only for a legitimate business reason, such as treating your own patients.

Privacy

Use and release of PHI

Patients receiving medical care expect privacy whether they are in a hospital, a physician's office, a laboratory, or other settings, including their homes. 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.

Privacy is essential to a healthcare provider's mission, and it's important to its patients as well. You must protect privacy as you perform your job. Remember that you don't want to interfere with patient privacy or jeopardize the confidentiality of patient information as you perform job-related tasks or work to meet deadlines.

Treatment, payment, and healthcare operations

HIPAA is not intended to interfere with providing patient care or receiving payment for it. Therefore, HIPAA permits your organization to use and release PHI for several reasons without patient permission. The most common reasons are to provide treatment, obtain payment, and perform certain healthcare operations (e.g., accreditation and peer review). These activities do not require any patient permission.

Other permitted uses and disclosures of PHI

HIPAA also permits release of PHI for special purposes and when required by law, without a patient's permission. Ensure that you know your organization's policies before releasing information, and confirm

that your situation is applicable and approved. In most cases, your facility is required to maintain a record of these releases. When in doubt, consult your privacy officer before releasing information that is not authorized in writing by the patient or legal representative.

Examples of scenarios in which your organization may be permitted or required to release PHI without patient permission 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 department of human services
- 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 (e.g., patients with gunshot wounds or burns that may be due to arson)
- Providing information to coroners or funeral directors when patients die

- 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

Disclosure of PHI to patients' families and friends

HIPAA requires you to obtain permission from a patient before discussing a patient with family members, friends, caregivers, and clergy members. This rule applies to providing the patient's medical information, demographic information (e.g., an address), and financial information. Normally, this requires that the patient sign an authorization form. However, if the individual is involved in the patient's care or in payment for the patient's care, HIPAA permits less formal permission from the patient, but it must be documented and limited to the minimum necessary information.

If a patient is unable to give permission, the caregiver should identify the next of kin, surrogate, power of attorney, or healthcare proxy, if any of these exists. If not, providers may use their professional judgment. PHI should not be released when a patient has indicated that an individual not receive personal information.

HIPAA and minors

HIPAA primarily relies on state law with respect to defining minors and to specifying when minors must give permission to providers before releasing their PHI to parents or guardians. As a general rule, if a minor may consent for treatment in your state, the minor must also sign an authorization to release documentation about the treatment.

HIPAA Handbook

for Home Health 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
- 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.

HHHHS2

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

ISBN: 978-1-61569-237-8
90000
9 781615 692378