HCPro

Omnibus Rule Update

HIPAA Handbook

for Behavioral Health Staff

Understanding the Privacy and Security Regulations

Kate Borten, CISSP, CISM

HIPAA Handbook for Behavioral Health Staff

Understanding the Privacy and Security Regulations

HCPro

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

ISBN: 978-1-61569-216-3

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
22022

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 Behavioral Health Staff
Understanding the Privacy and Security Regulations

Intended Audience

This handbook explains the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules as applicable and relevant to behavioral health staff. It also addresses the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 privacy, security, and breach notification provisions and 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 (Omnibus Rule). Case scenarios will illustrate potential situations in which privacy and security may be breached.

The intended audience includes the following:

- Nurses
- Mental health professionals
- Medical records, patient accounting, registration, and back office staff

- Dietary services staff
- Housekeeping/facilities staff
- Trainees, students, and volunteers
- All other ancillary staff

Learning Objectives

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
- Describe protected health information and explain why protecting patient privacy is important
- Explain patient rights for accessing their medical information and other rights they have regarding their protected health information
- Determine when disclosures of protected health information are acceptable
- Summarize how to protect confidential health information by following proper security procedures in the organization and off-site
- Create effective passwords to protect electronic information
- Know how to identify and report privacy and security incidents

Health Information Privacy and Security

Most healthcare organizations have always upheld strict privacy and confidentiality policies, but there was no federal law and not every state had laws to protect the privacy of patient information and give patients rights.

With the enactment of HIPAA, the right to have one's health information remain private and secure became more than just an ethical obligation—it became federal law, with civil and even criminal penalties for violations.

HIPAA Basics

What is HIPAA?

HIPAA is a 1996 federal law that establishes the basic privacy protections to which all patients in the United States 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.

To make it easier and more efficient for healthcare organizations to share medical information, the law requires that common electronic transactions—such as submitting a claim on the patient's behalf—be in a standard format for all healthcare organizations and payers. But as patient information becomes easier to transmit, it also becomes easier for information leaks and abuses to happen. This is especially true as more information is shared electronically through email and the Internet.

Under HIPAA, it is illegal to release health information to inappropriate parties or to fail to adequately protect health information from unauthorized release. Organizations may face significant fines, and individuals can even receive prison terms for violations of HIPAA, especially if the violations are deliberate. As you read this handbook, you will notice that privacy and security are directly related, because the security measures discussed protect privacy and confidentiality.

What are the HITECH Act and the Omnibus Rule?

The American Recovery and Reinvestment Act of 2009 includes the HITECH Act, which requires heightened enforcement of HIPAA and stiffer penalties for privacy and security violations. It also expands the HIPAA Privacy Rule and Security Rule to strengthen patient privacy. Examples include the following:

- Increasing HIPAA's patient rights regarding control of protected health information
- Limiting use of protected health information for marketing purposes
- Mandating breach notification to patients and the government
- Protecting protected health information by explicitly requiring business associates to comply
- Requiring covered entities to comply with patients' requests for restrictions on disclosure in certain circumstances (previously this was optional)

The 2013 Omnibus Rule implements many of the HITECH Act provisions for protected health information protection, 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 behavioral health facilities, physician practices, therapists, dental practices, hospitals, ambulatory facilities, skilled nursing facilities, home health agencies, and pharmacies. The organization you work for is a CE and must comply with these rules.

Protected health information or PHI

HIPAA sets 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. But 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 the 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.

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. 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 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 people with an authorized "need to know" to perform their jobs may have access to PHI. HIPAA requires healthcare workers to use and share or release only the minimum necessary information to perform their jobs without compromising patient care.

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

- Do I need this information to do my job?
- What is the least amount of information I need to perform my job?
- Does the other person need this information to perform his or her job?

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 Disclosure 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 organizations 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, as well as when required by law.

Examples of scenarios in which your organization may be subject to laws and regulations permitting or requiring release of PHI include the following:

- Reporting certain communicable diseases and other conditions to public 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 (e.g., individuals with gunshot wounds or burns that may be due to arson)
- 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
- Providing information to coroners and funeral directors when patients die

The Omnibus Rule adds another public health situation not requiring formal authorization. Providers now are permitted to release a student's immunization status to schools when schools are required by law to obtain that information and when there is informal agreement, such as a telephone call from a parent. Providers must limit the disclosure to immunization status only and must document the agreement from the parent, guardian, or adult student.

Always be sure you know your organization's policies before releasing information, and ensure that each release is approved. Remember the following motto, "When in doubt, don't give it out," unless you first check with your supervisor or the privacy officer.

Family and friends

HIPAA requires you to obtain permission from a patient before disclosing PHI to family members or friends. In the case of someone who is involved in a patient's care or payment for that care, permission may be informal and does not require an authorization but should be documented. Patients should be given an opportunity to agree or object to sharing their PHI with such individuals. Professional judgment may be used in certain situations to determine a patient's wishes.

The Omnibus Rule adds that when a patient is deceased, the CE may disclose to such family members or others the PHI that is relevant to their involvement in care or payment. However, the CE should not disclose PHI if it knows that the deceased patient had expressed a preference for not disclosing the PHI to an individual.

Conversely, a patient's PHI should not be disclosed to other friends or family members who are not involved in a patient's care or payment unless the patient has signed an authorization form. If you don't have specific authorization to disclose additional PHI or to disclose PHI to family members and friends who are not involved in a patient's care or payment for services, restrict the information to that which is included in the patient directory (typically location in the facility, telephone extension, and general condition). If a patient has opted out of being listed in the facility directory, you may not disclose even this information.

You may be responsible for keeping track of identifying and recording when patients agree to or forbid specific disclosures to family members, friends, or other caregivers. Document these patient decisions carefully

and pass them on to the appropriate staff member as necessary to ensure that they are followed.

In all cases, ensure that you know the policy before releasing any patient information. If in doubt, consult your privacy officer.

HIPAA authorizations

CEs are permitted to use and release PHI for treatment, payment, and healthcare operations, as well as for public health and other purposes serving the public good without first obtaining an authorization—formal written permission—from patients. HIPAA's Privacy Rule explains other special situations when CEs must give patients an opportunity to agree or disagree with the way their PHI is used or released but that do not require a formal authorization.

However, for any other use or disclosure of PHI, CEs first must ask patients, or their legal representatives, for their authorization. With an authorization, the patient voluntarily agrees to let your organization use or release the information for a particular need.

A valid HIPAA authorization form must be completed with the following information:

- A description of the specific PHI to be used or disclosed
- The reason or purpose for this use or disclosure
- The party to whom the PHI will be released

HIPAA Handbook for Behavioral 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:

- 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
- Registration and front office staff

HHBHS2

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

ISBN: 978-1-61569-216-3