HCPro

Omnibus Rule Update

HIPAA Handbook for Business Associates

Understanding the Privacy and Security Regulations

Kate Borten, CISSP, CISM

HIPAA Handbook for Business Associates

Understanding the Privacy and Security Regulations

HCPro

HIPAA Handbook for Business Associates: Understanding the Privacy and Security Regulations is published by HCPro, Inc.

ISBN: 978-1-61569-225-5

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
22032

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 Business Associates
Understanding the Privacy and Security Regulations

Intended Audience

You work for an organization that is designated as a business associate (BA) of one or more Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities (CE) or of another BA. This means your organization provides some service for or on behalf of a healthcare provider or payer, directly or indirectly, and that service involves access to protected health information.

Many kinds of organizations can be designated as BAs, including the following:

- Certain consulting firms
- Coding and billing services
- Transcription services
- Collection agencies
- Record/data storage and disposal companies

- Certain attorneys and auditors
- Professional management services
- Electronic health record vendors
- Certain personal health record vendors
- Information technology (IT) management and support companies, including cloud vendors
- Health information organizations and regional health networks
- E-prescribing gateways
- Patient safety organizations
- Accreditation agencies

Learning Objectives

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

- Understand what HIPAA and the Healthcare Information Technology for Economic and Clinical Health (HITECH) Act are and how they affect BAs and their workforce
- Understand what constitutes protected health information
- Protect patient privacy while performing BA-related tasks

- Recognize the permissible uses and disclosures of protected health information
- Identify safe ways to handle email and faxes containing PHI
- Protect protected health information both inside the organization and off-site
- Create effective passwords to protect electronic information

HIPAA, the HITECH Act, and Omnibus Rule Overview

HIPAA requires privacy and security protections for individually identifiable patient and health plan member information or protected health information. The HIPAA Privacy and Security Rules require CEs to have special contracts with their BAs to pass on many of these obligations, making BAs contractually liable.

The American Recovery and Reinvestment Act of 2009 includes a subset called the HITECH Act, which, extends direct liability to BAs for compliance with HIPAA's Security Rule and certain portions of HIPAA's Privacy and Breach Notification Rules. Until enactment of the HITECH Act, the U.S. Department of Health and Human Services (HHS) could enforce only CEs' compliance with HIPAA rules. Now BAs have both direct liability to the federal government and contractual liability to the CE with which it signed a BA contract.

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) makes BAs directly liable for the following:

- Failure to comply with the HIPAA Security Rule
- Uses and disclosures of protected health information that are impermissible according to the HIPAA Privacy Rule
- Failure to provide access to electronic protected health information when requested by the individual who is the subject of the protected health information, or by the relevant CE on behalf of the individual
- Failure to provide an accounting of certain protected health information disclosures as required by the Privacy Rule
- Failure to provide breach notification as required by the Breach Notification Rule
- Failure to provide protected health information to HHS when required by an investigation or to determine the BA's compliance

The HITECH Act further includes provisions for heightened enforcement of HIPAA and stiffer penalties for noncompliance and privacy and security violations. It also is the first federal law to require notification in case of a breach of a patient's or plan member's information.

The 2013 Omnibus Rule implements many of the HITECH Act requirements and goes further. Directly relevant to BAs, the Omnibus

Rule expands the definition of a BA to include all of a BA's downstream subcontractors with access to protected health information. BAs generally are required to pass along the same contractual obligations and limits to its downstream subcontractors that it has to its upstream BAs or CEs. Note that the Omnibus Rule revises some required language in BA contracts.

Your organization must ensure that HIPAA-compliant BA contracts are signed before permitting another person or entity to have access to protected health information for which you are responsible. Contracts must specify that subcontractors will do the same if they subcontract. If a subcontractor discovers a privacy or security incident or breach, the incident must be reported up the chain to the affected CEs.

HIPAA and you

As a BA, you might have access to protected health information, you might have a business need to discuss protected health information with colleagues and third parties, and you might communicate with patients or health plan members and even members of their families. The HITECH Act and Omnibus Rule changes make understanding HIPAA privacy and security requirements particularly important.

Terms You Should Know

Protected health information or PHI

HIPAA and your organization's BA contracts establish rules for when and how protected health information or PHI may be used and released. So it is essential to understand what constitutes PHI.

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. However, information without obvious identifiers can still point to one individual. For example, if only one patient underwent a particular medical procedure this week, the procedure would be enough to identify that patient and would be PHI. Alternatively, if only one health plan member is a goat herder residing in New York City, this occupation combined with residence would be enough to identify this individual.

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 and insurance claims information, insurance eligibility and coverage, the reason a person is sick or in the hospital, treatments and medications a patient may receive, test results, photographs and radiology images, allergies, observations about a patient's condition, information about past health conditions or treatments, discharge planning information, and more. The Omnibus Rule explicitly adds genetic information about individuals and their family members to the definition of PHI.

Minimum necessary/need to know

HIPAA requires that BAs follow the principle of minimum necessary when using, disclosing, and requesting PHI. Otherwise, it is an impermissible use, disclosure, or request under the Privacy Rule.

Only individuals with an authorized "need to know" to perform their jobs may have access to PHI. Furthermore, individuals with access to PHI may access and release only the minimum necessary PHI to perform their jobs.

Your use and disclosure of PHI must also comply with your organization's BA contracts. BA contracts specify which functions or services your organization is performing that put your organization in contact with PHI. Other than performing these functions or services, there are limited other purposes for which your organization is permitted to use or disclose PHI. You must ensure that you access and release PHI only as permitted by your organization's contracts and policies.

Ask yourself the following questions before you access 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?
- To whom am I releasing the information, and is that person or entity permitted to have it?
- Does this use or disclosure comply with HIPAA and our BA contracts?

Ensure that you release only the minimum necessary PHI in response to a request or to serve a particular purpose. When you release PHI, even if another party has requested more PHI, your organization is responsible if the PHI is excessive. Violation of the minimum necessary principle is a HIPAA violation and can result in federal penalties for BAs. If you are

unsure about a certain situation, consult your privacy officer, compliance officer, or information security officer (ISO).

Case scenario #1: Celebrity sighting

You work for a billing company and you are preparing a patient bill when you recognize the patient's name—he's the shortstop for the Chicago Cubs. Apparently, physicians at the hospital for which your company provides billing services performed an outpatient procedure on his shoulder.

During a break later in the day, you call a friend who works at the hospital to learn more about the famous patient. She cared for the patient and discusses his condition. You chat for a few more minutes, but you think about the conversation as you prepare to return to work.

The conversation was not malicious, and it was between friends, so it seems harmless. But something tells you it was inappropriate.

Did you do anything wrong?

Yes. You and your friend violated HIPAA, and this was potentially a breach. You must report it to your supervisor, privacy officer, or other designated leader for investigation. You regret that it happened and you realize that you had no business inquiring about the patient because it had nothing to do with your job. Your friend made matters worse because she should not have told you that she cared for this celebrity or discussed him with you. This is a HIPAA privacy violation, despite your belief that the conversation was harmless.

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 and physicians accessed the patient's information strictly out of curiosity, not for a work-related need. Disciplinary action ensued, and the facilities involved endured public embarrassment.

Privacy Rights of Patients and Health Plan Members

BAs are both directly liable and contractually liable for supporting certain privacy rights of individuals.

Access to one's PHI

Patients and plan members generally have a right to view and receive a copy of their PHI in a designated record set. Each BA and CE or upstream BA must agree contractually whether the BA has PHI in a designated record set as determined by the original CE and, if so, how and by whom requests for access and copies will be handled. The Omnibus Rule strengthens individuals' right to receive electronic copies when PHI is in electronic form, and the right to have their PHI transmitted, in any form, to a third party.

Amending PHI

Patients and plan members have a right to request amendments to their PHI. Unlike updating an address or insurance plan, this refers to amending substantive information, particularly when relevant to a

patient's care. For example, a patient may view his or her medical record and notice that a laboratory test is missing or incomplete. The patient may then request that an amendment be added to the record. CEs are not required to agree, but if they do, the PHI held by BAs may require amendment. BAs and CEs should agree on procedures for this situation.

Restrictions on PHI use and disclosure

Patients and plan members have a right to request restrictions on how their PHI is used and disclosed or to whom. Generally, CEs are not required to agree. However, the Omnibus Rule requires healthcare providers to agree when a patient requests that a claim not be submitted for a service or item for which the patient pays in full out of pocket. Any restriction that a CE agrees to must be strictly upheld. Some restrictions may affect BAs; they and CEs should agree on how to respond when this occurs.

Accounting of disclosures

Patients and plan members have a right to request and receive an accounting of certain PHI disclosures occurring during the previous six years. This accounting or report excludes disclosures for treatment, payment, healthcare operations, and disclosures the patient or plan member has authorized. Many possible disclosures must be tracked (e.g., disclosures made for public health purposes). BAs are directly responsible for knowing which disclosures require tracking and, if relevant to the BA's circumstances, tracking all such disclosures. Furthermore, BAs must have an on-demand retrieval and reporting process to respond within 60 days of an individual's accounting request.

HIPAA Handbook for Business Associates

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
- 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

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.

HTHBA2

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

ISBN: 978-1-61569-225-5