HCPro

THE HIPAA OMNIBUS RULE TOOLKIT

A Covered Entity and Business Associate Guide to Privacy and Security

KATE BORTEN, CISSP, CISM

The HIPAA Omnibus Rule Toolkit

A Covered Entity and Business Associate Guide to Privacy and Security

Kate Borten, CISSP, CISM

HCPro

The HIPAA Omnibus Rule Toolkit: A Covered Entity and Business Associate Guide to Privacy and Security is published by HCPro, Inc.

ISBN: 978-1-61569-271-2

Kate Borten, CISSP, CISM, Author
Gerianne Spanek, Managing Editor
Erin Callahan, Senior Product Director
Melissa Osborn, Product Director
Mike Mirabello, Production Specialist
Matt Sharpe, Senior Manager of Production
Shane Katz, Art Director
Jean St. Pierre, Vice President, Operations and Customer Relations

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
E-mail: *customerservice@hcpro.com*

Visit HCPro online at: *www.hcpro.com* and *www.hcmarketplace.com*.

08/2013
53589

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 (MGH), where she was responsible for system development. As the trend shifted from building to buying new systems, Borten's role evolved into management of major projects, integrating legacy and vendor systems across various technical platforms at MGH, which includes a Harvard University–affiliated medical center, research laboratories,

psychiatric and rehabilitation hospitals, community health centers, and a physician network. As care delivery and reimbursement in the United States underwent radical change, she led and consulted on strategic multidisciplinary projects that demonstrated her management skills and her ability to rapidly assimilate and apply new technologies to meet business objectives.

When the quantity and accessibility of electronic patient-identifiable heath data grew during the 1990s, the healthcare industry began to take serious notice of patient confidentiality and security issues. Borten managed and developed MGH's first information security program, including policies, procedures, technical controls, and workforce privacy and security education.

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.

Borten 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. Borten served on the Massachusetts Health Data Consortium confidentiality committee and serves as an advisor and contributor to HIPAA and health information security and privacy newsletters, including *Briefings on HIPAA* published by HCPro, Inc.

Borten is the author of *The HIPAA Omnibus Rule: A Compliance Guide for Covered Entities and Business Associates, The No-Hassle Guide to HIPAA Policies: A Privacy and Security Toolkit, HIPAA Security Made Simple: Practical Advice for Compliance*, and *HIPAA Security Made Simple for Physician Practices: Practical Compliance Advice for Small Offices*, all published by HCPro.

Borten attended Vanderbilt University and received a BA in mathematics from Boston University. She has completed additional technical and management programs and studied data communications at Harvard University.

CD-ROM CONTENTS

The HIPAA Omnibus Rule Toolkit: A Covered Entity and Business Associate Guide to Privacy and Security provides policies, forms, and other information designed for use in addition to policies and tools you may already have. It is not intended to provide everything you need to ensure complete HIPAA compliance at your organization.

Note that the information in this toolkit is neither intended as nor should it be considered legal advice. It is intended to be adapted to meet the specific needs of your organization.

HIPAA Reference Tools

1. **Glossary of Selected HIPAA Terminology.** This document includes the definitions of key legal terms used in HIPAA. These terms can be included in relevant privacy and security policies. Alternatively, policies can refer to a separate glossary for an explanation of these important terms.

2. **HIPAA Security Rule Matrix.** Most of the HIPAA Security Rule's standards and implementation specifications are summarized in an appendix to the rule, commonly referred to as the *matrix*. This document includes the matrix and additional Security Rule requirements, including detailed information from the Code of Federal Regulations.

3. **HIPAA/HITECH Act Administrative Simplification Penalties.** These tables summarize the civil and criminal penalties for violation of HIPAA privacy and security regulations.

Managing Business Associate and Subcontractor Relationships

These documents help organizations manage the legally mandated relationships between covered entities (CE) and business associates (BA) and between BAs and their protected health information (PHI)–related subcontractors.

4. **Business Associate Contracts: Sample Business Associate Agreement Provisions** is the model provided

by the U.S. Department of Health and Human Services during January 2013. This is not a comprehensive legal contract; organizations should always consult legal counsel with respect to business contracts. This is a new contract for BAs to use with subcontractor BAs. CEs should already be using BA contract templates that meet HIPAA requirements; they can add language to meet Omnibus Rule requirements. This document or the associated services contract must be customized to reflect the particular services a BA or a BA's subcontractor is intended to provide. In certain CE–BA and BA–BA relationships, some patient privacy rights (e.g., access and accounting of disclosures) must be extended to a downstream BA, but in others they are moot. In all cases, the BA must agree to limit PHI uses and disclosures to that which HIPAA allows.

5. **Business Associate Tracking.** Contracts (or other legal arrangements when government agencies are involved) are required. This spreadsheet helps CEs and BAs identify every BA, the services each BA provides, and the date each contract was signed and by whom. Ensure that signers have legal authority.

6. **Questions to Ask When Selecting Business Associates.** The extent to which CEs and BAs actively oversee BA compliance varies widely, generally depending on the organization's resources and risk tolerance. This document suggests questions that a CE or BA should ask a potential BA or subcontractor BA.

Breach Notification Preparation

Breach notification is increasingly important at the state and federal levels. Breach determination and notification preparedness should be part of every CE's and BA's incident response plan. These documents help organizations proactively prepare breach response procedures.

7. **Breach Determination: Final Breach Notification Rule.** This document illustrates the decision-making process for determining whether a HIPAA breach that requires notification has occurred. A privacy/security incident may be a breach of PHI subject to notification under HIPAA, and/or the incident may be in violation of state law. Ensure that you understand how each

applicable state breach notification law defines personal data that are subject to the law.

8. **HIPAA Breach Notification Checklist.** If a breach of PHI occurs, this checklist helps ensure compliance with Breach Notification Rule requirements.

Security

This CD-ROM includes the following sample policies and forms to jump-start your program:

9. **Confidential Data Protections Policy.**
10. **Security of Portable Computing Devices and Media Policy.**
11. **Off-Site User Device Inventory Form.** This document should be used for portable devices and desktop computers that are used off-site.
12. **Encryption of Confidential Information Policy.**
13. **Disposal Policy Statement.**

14. **Off-Site Computers and Media Security.**

15. **Working Off-Site Security Agreement.**

16. **Privacy and Security Training PowerPoint® Presentation.** CEs and BAs are required to provide privacy and security training to their workforce members. At the simplest level, workforce members must understand the risks, organization rules, and the consequences of violations. This slide presentation can help organizations implement training programs.

THE HIPAA OMNIBUS RULE TOOLKIT

A Covered Entity and Business Associate Guide to Privacy and Security

KATE BORTEN, CISSP, CISM

The HIPAA Omnibus Rule is a compilation of new HIPAA privacy and security regulations, long awaited by the healthcare industry and supporting businesses. This toolkit updates ***The HIPAA and HITECH Toolkit*** to help covered entities and business associates understand and comply with the new requirements.

This toolkit explains HIPAA terminology and provides information about the Security Rule, the Breach Notification Rule, and Administrative Simplification Penalties. It includes information about selecting and tracking business associates and a sample agreement. It also includes a PowerPoint® training presentation and sample policies pertaining to confidential data protection, security of portable devices, encryption of confidential information, off-site computers and media security, and disposal of confidential materials.

HBAT2

ISBN: 978-1-61569-271-2

HCPro

75 Sylvan St., Suite A-101 | Danvers, MA 01923

www.hcmarketplace.com