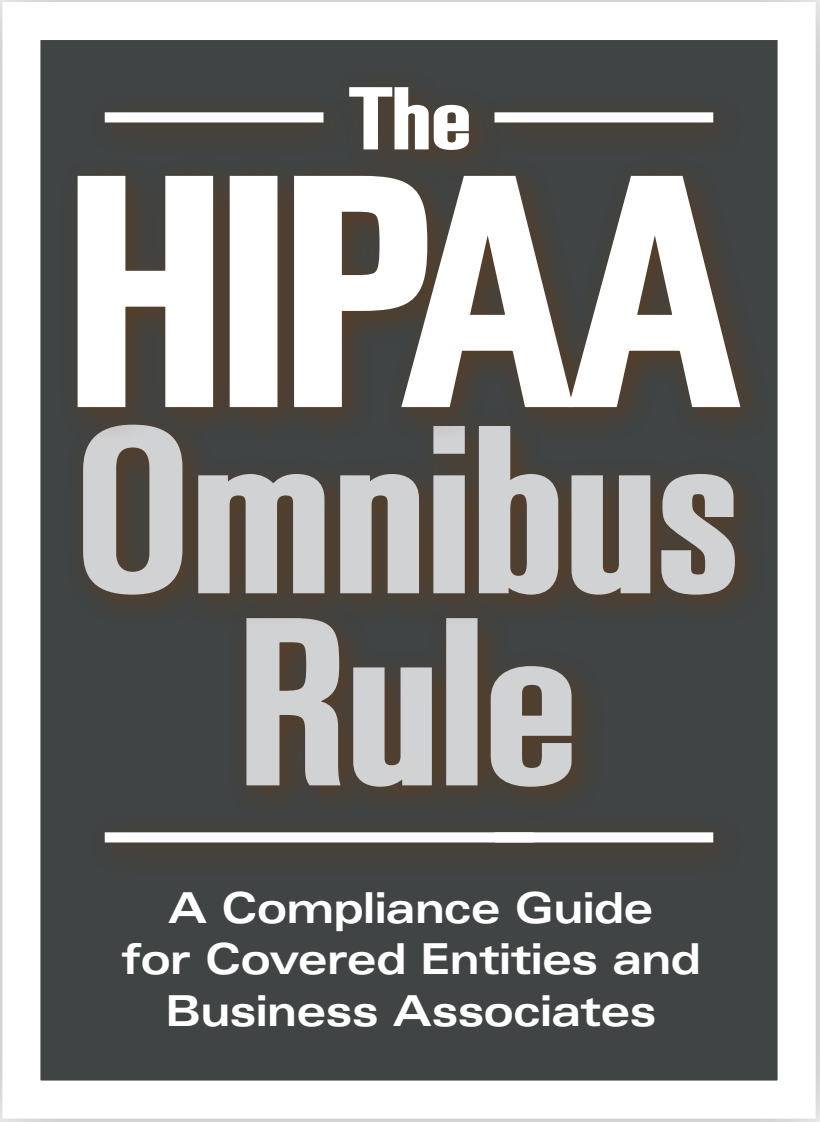
The HIPAA Omnibus Rule

A Compliance Guide for Covered Entities and Business Associates

Kate Borten, CISSP, CISM



Kate Borten, CISSP, CISM

HCPro

The HIPAA Omnibus Rule: A Compliance Guide for Covered Entities and Business Associates is published by HCPro, Inc.

ISBN: 978-1-61569-214-9

Kate Borten, CISSP, CISM, Author
Gerianne Spanek, Managing Editor
James T. DeWolf, Publisher and Editorial Director
Mike Mirabello, Production Specialist
Matt Sharpe, Senior Manager of Production
Shane Katz, Art Director
Jean St. Pierre, Vice President, Operations and Customer Relations

For more information, contact:

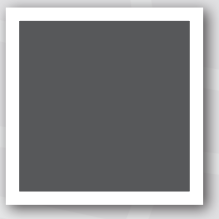
HCPro, Inc.
75 Sylvan Street, Suite A-101
Danvers, MA 01923
Telephone: 800-650-6787 or 781-639-1872
Fax: 800-639-8511
Email: *customerservice@hcpro.com*

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

05/2013
22034

Contents

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 (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 health 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.

ABOUT THE AUTHOR

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. She is the author of *The No-Hassle Guide to HIPAA Policies: A Privacy and Security Toolkit, HIPAA Security Made Simple,* and *HIPAA Security Made Simple for Physician Practices,* all published by HCPro, Inc.

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.

Introduction

The U.S. Department of Health and Human Services (HHS) published a final rule titled "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; Other Modifications to the HIPAA Rules" January 25, 2013, in the Federal Register. Due to its lengthy title and broad scope, it is commonly called the HIPAA (Health Insurance Portability and Accountability Act) Omnibus Rule.

The Omnibus Rule revises 45 CFR (Code of Federal Regulations) Parts 160 and 164. Part 160 includes definitions of important terms for HIPAA administrative simplification, such as business associate (BA) and genetic information. It also includes revised penalties and enforcement details. Part 164 includes the Security, Privacy, and Breach Notification Rules.

The Omnibus Rule modifies the Breach Notification Rule, replacing the 2009 final interim rule. It increases privacy protections for genetic information as required by the Genetic Information Nondiscrimination Act of 2008 (GINA) and for other protected health information (PHI) used for purposes including marketing and underwriting. It extends liability for compliance to BAs.

The Omnibus Rule was years in the making, with many of the changes mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act. It comprises numerous small adjustments for accuracy, clarity, and consistency across the affected rules (i.e., Privacy, Security, Breach Notification, Enforcement). It modifies the definitions of critical terms, including PHI, BA, and marketing. It also includes several sweeping changes likely to affect the entire healthcare industry.

Most of the Omnibus Rule's changes and new requirements are enforceable September 23, 2013. (Exceptions are discussed elsewhere in this book.) Failure to comply by this date can lead to civil and even criminal penalties for covered entities (CE) and BAs.

This book provides a reader-friendly summary of the changes brought about by the rule, explains the intent and impact of each change, and provides strategies for compliance. Some changes affect only CEs or only a subset of CEs, some affect BAs, and some affect the full range of these organizations. The compliance strategies for each provision indicate which organizations are subject to civil liability for compliance. Every BA that performs a function related to the change will have at least contractual liability and, in some cases, civil liability also.

Chapter 1 provides an overview of techniques for managing the required security and privacy programs and project management necessary to achieve regulatory compliance. Chapter 2 explains two changes to the definition of PHI; every healthcare organization should note this important information. Chapter 3 explains which entities will become BAs under the Omnibus Rule and clarifies specific categories of BAs (e.g., patient safety organizations). Because the HITECH Act makes BAs directly liable for compliance, understanding which organizations qualify as BAs has never been more important. Chapter 4 focuses on the new content of contracts with BAs and the rule's impact on data use agreements. Chapter 5 clarifies two important new privacy rights and how organizations must prepare for them. Chapter 6 explains new limitations pertaining to fundraising, marketing, sale of PHI, and underwriting activities. Chapter 7 explains the easing of privacy protections for the purposes of research, reporting student immunization status, and family access to decedents' PHI. Chapter 8 explains the Breach Notification Rule changes that affect all CEs and BAs. Chapter 9 identifies which of the Omnibus Rule changes are material and, thus, require changes to CEs' privacy notices. Chapter 10 discusses changes to the Enforcement Rule, including tiered penalties for noncompliance.

The online Appendix glajsbcq rfc dmjjmugle:

- Information about BA contracts and sample contract language from HHS
- A user-friendly chart that lists the civil penalties for failure to comply with the Privacy, Security, Breach Notification, and other HIPAA administrative simplification rules
- A Law Finder with links to the Electronic Code of Federal Regulations (Title 45, Parts 160 and 164) and the January 25, 2013 Federal Register
- An Omnibus Rule Compliance Tracker that maps compliance steps to specific regulations and the chapters in this book that address them

INTRODUCTION

This book provides a thorough compilation of the Omnibus Rule changes of which CEs and BAs must be aware. However, it doesn't include all changes (e.g., many are housekeeping changes intended to synchronize the rules and adjust citations).

Editor's note: The informal term "Omnibus Rule" is used throughout this book in place of 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; Other Modifications to the HIPAA Rules. The term "person," which is used throughout the Omnibus Rule, means an individual or an entity. Internet links to government websites included in this book and its online Appendix are provided as a convenience, with no guarantee that they will be accessible in perpetuity.

DOWNLOAD YOUR MATERIALS NOW

Readers of *The HIPAA Omnibus Rule: A Compliance Guide for Covered Entities and Business Associates* can download the online Appendix that accompanies this book. Visit the HCPro website below:

Uc`qgrc _t_gj_`jc snml nspaf_qc md rfgq npmbsar,

Thank you for purchasing this product!

HCPro

1 Compliance Strategies

Information privacy and security programs must be dynamic and open-ended. There is no such thing as a risk-free environment, especially when humans are involved. Realistically, there is no ultimate end state that, when reached, allows us to sit back, relax, and let these programs manage themselves.

Conversely, dynamic programs include projects with discrete milestones and end goals. When presented with new regulations such as the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule, organizations are faced with a compliance project.

Good project management starts with identifying and documenting project leaders, the scope of the project, and its end goals. Project leaders in this case could be an organization's privacy (or compliance) and security officials because they are typically the subject matter experts. Once appointed, project leaders should form a team or, in larger organizations, a steering committee and working groups.

The project team should include or involve stakeholders and knowledge holders. Because documentation is critical to regulatory compliance, the team should also include a scribe or a document taskmaster to ensure recording of the full process and deliverables as necessary. Along the way, organizations can draw on internal and external resources such as this book, consulting services, and government websites (e.g., *http://csrc.nist.gov*) for guidance and support.

An organization's documentation should demonstrate that it reviewed the Omnibus Rule and identified relevant regulatory changes. Achieving rule compliance may necessitate updating policies and procedures; revising, mailing, and posting covered entities' privacy notices; developing or revising and signing business associate contracts; and providing workforce training to explain changes relevant to the organization.

Steps taken to comply with each change should be project tasks with incremental milestones. Documentation should reflect who performed each task, when, and the outcome (e.g., decisions made, documents created or revised, training provided). Tangible deliverables (e.g., new policy or training presentation) should also be documented along with the effective date. Maintain such documentation where it is easily retrievable when necessary for internal and external audits. Satisfying HIPAA document retention requirements entails retention of earlier versions of policies, training materials, and other documentation for six years after the date new versions superseded them.

This book includes suggestions for compliance with each requirement discussed. The online Appendix also includes a downloadable electronic spreadsheet that maps rule topics to citations and compliance steps discussed in the book. This tool can help organizations track progress, status, and additional items, such as task assignment and deliverables.

2 The Evolving Definition of PHI

Genetic Information

Editor's note: Refer to chapter reference 2A in the Omnibus Rule Compliance Tracker in the online Appendix.

Genetic information is protected health information (PHI).

The Genetic Information Nondiscrimination Act (GINA) of 2008 defines genetic information and requires that it be protected. The Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule explicitly includes genetic information in the definition of health information, which is part of the definition of PHI.

The Code of Federal Regulations at 45 CFR 160.103 [Definitions] defines genetic information, services, and tests as follows:

> Genetic information means
>
> (1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:
>
> (i) The individual's genetic tests;
>
> (ii) The genetic tests of family members of the individual;
>
> (iii) The manifestation of a disease or disorder in family members of such individual; or
>
> (iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman;

and

(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual.

Genetic services means:

(1) A genetic test;

(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

(3) Genetic education.

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

The rule at 45 CFR 160.103 further defines family member as follows:

Family member means, with respect to an individual:

(1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or

(2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Understanding what these definitions include is important for ensuring that genetic information remains confidential and is not used for underwriting purposes.

Long-Deceased Individuals

Editor's note: Refer to chapter reference 2B in the Omnibus Rule Compliance Tracker in the online Appendix.

Long-deceased individuals' health information is not PHI.

Before the Omnibus Rule, PHI included the health information of deceased persons. The Omnibus Rule modifies the applicability of HIPAA protections to exclude the individually identifiable health information of a person who has been deceased for more than 50 years.

The rule at 45 CFR 160.103 states:

Protected health information excludes individually identifiable health information … [r]egarding a person who has been deceased for more than 50 years.

Less restrictive protection of the health information of long-deceased individuals should reduce the compliance burden on covered entities (CE) and business associates (BA). It should also make retrospective historic record research easier.

Note that other laws may be more stringent. For example, a state law that requires protection for individually identifiable information indefinitely supersedes this change. Also note that this HIPAA regulatory change does not affect laws that govern medical record retention.

COMPLIANCE STEPS

The following compliance steps apply to CEs and BAs.

1. Document

Organizations can ensure consistency and clarity by developing a readily accessible glossary of terms that are frequently used in their policies and procedures. This eliminates the need to repeat definitions in each document and avoids the risk of inconsistency.

HIPAA compliance requires an accurate understanding of many key terms. One is protected health information or PHI.

Revise your organization's glossary definition of PHI so that it includes genetic information and excludes the PHI of individuals deceased for more than 50 years. Record the date of the revision. Because the definition of PHI incorporates these terms, add or revise your definitions of genetic information, genetic services, genetic test, and family members to comply with the new regulations.

2. Review

Review organization research policy and procedures. Consider amending them to explicitly permit historic records research on individuals who have been deceased for more than 50 years without requiring authorization unless your organization is subject to more stringent state law. Note that although HIPAA permits this under the Omnibus Rule, organizations are not required to remove protections from these records.

3. Train

Provide workforce training to explain that genetic information is PHI. Include examples of genetic information, services, and tests in the context of your particular organization to demonstrate the scope of genetic information.

GINA and the Omnibus Rule restrict health plans that use PHI to perform underwriting activities from the use and disclosure of genetic information for this purpose. Additional information and compliance steps appear in Chapters 6 and 9.

The HIPAA Omnibus Rule

A Compliance Guide for Covered Entities and Business Associates

Kate Borten, CISSP, CISM

Kate Borten, CISSP, CISM, an internationally certified information security professional, uses clear and concise language to explain 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; Other Modifications to the HIPAA Rules. This final rule, commonly referred to as the Omnibus Rule, revises the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules.

This easy-to-read guide describes the revisions and offers advice for complying with new requirements and standards. Almost every covered entity and business associate must revise its policies and procedures because of the Omnibus Rule. This book is your first step on the path to compliance.

- Information is presented in a user-friendly format that facilitates compliance with HIPAA Omnibus Rule requirements
- The author distills and summarizes the nearly 600-page Omnibus Rule and preamble published January 25, 2013, in the Federal Register
- Specific examples clarify how, when, and to whom various provisions of the Omnibus Rule apply
- The online Appendix provides instantaneous access to the Electronic Code of Federal Regulations
- The Omnibus Rule Compliance Tracker in the online Appendix facilitates compliance planning and management

The online Appendix includes these resources:

- Business Associate Contracts: Sample Business Associate Agreement Provisions
- HIPAA/HITECH Act Administrative Simplification Penalties
- Law Finder
- Omnibus Rule Compliance Tracker

Need to train your entire staff or organization?
Volume discounts are available for our ***HIPAA Training Handbook Series,*** which provides fundamental privacy and security training for workforce members with specific roles in various healthcare settings and business associates. Please call 877-233-8828 or email *sales@hcpro.com* for more information.

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

HOR

ISBN: 978-1-61569-214-9
90000
9 781615 692147