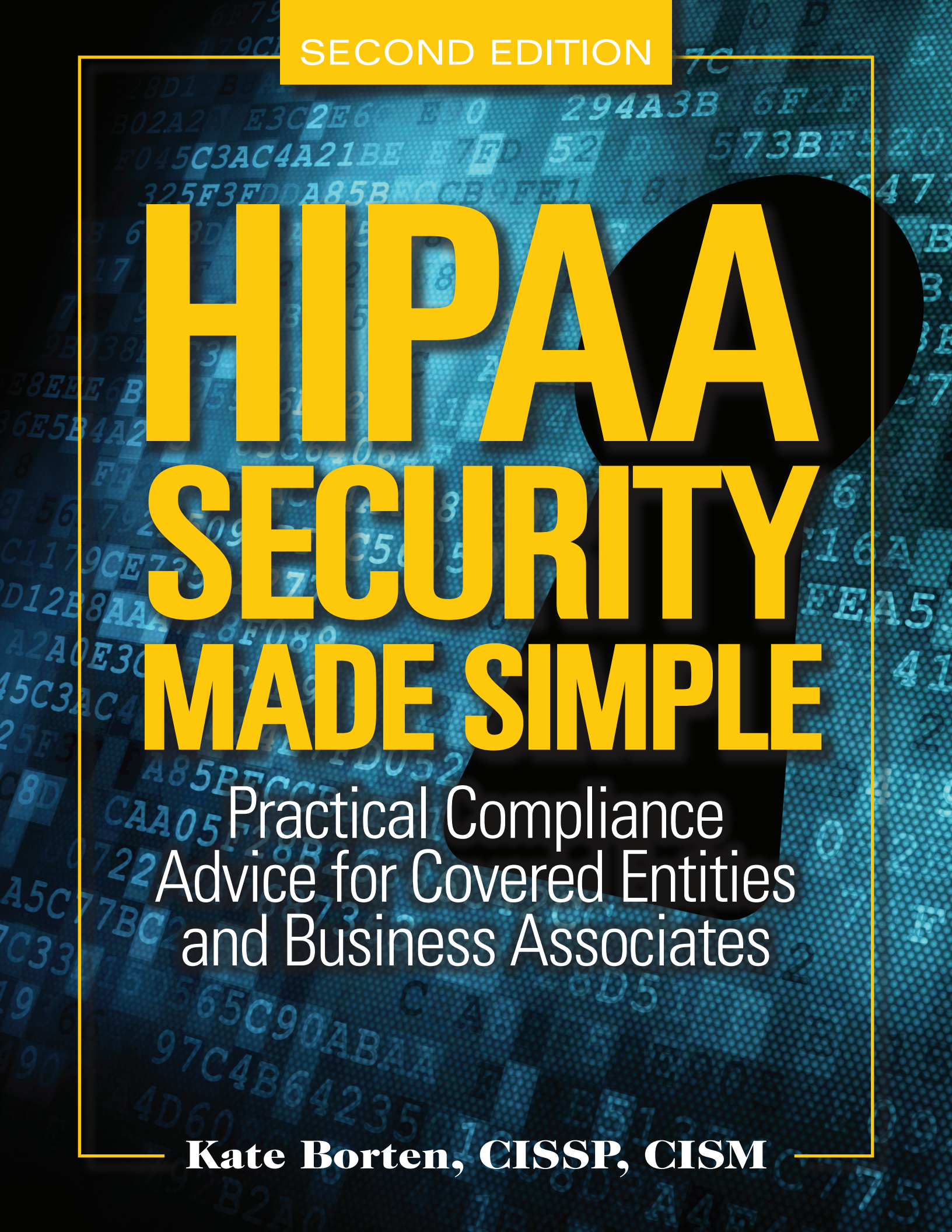

SECOND EDITION
HIPAA
SECURITY
MADE SIMPLE
Practical Compliance
Advice for Covered Entities
and Business Associates
Kate Borten, CISSP, CISM

SECOND EDITION

# HIPAA SECURITY MADE SIMPLE

Practical Compliance Advice for
Covered Entities and Business Associates

**Kate Borten, CISSP, CISM**

HCPro

*HIPAA Security Made Simple: Practical Compliance Advice for Covered Entities and Business Associates*, Second Edition, is published by HCPro, a division of BLR.



Download the additional materials of this book with the purchase of this product.

ISBN: 978-1-61569-273-6



HCPro, a division of BLR, provides information resources for the healthcare industry.

HCPro, a division of BLR, is not affiliated in any way with The Joint Commission, which owns the JCAHO and Joint Commission trademarks.

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
Elizabeth Petersen, Vice President

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, a division of BLR
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*.**

12/2013
22068

# Contents

**Access the online Appendix with the purchase of this product.**

# 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 Care-Group, 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, a division of BLR.

Borten is the author of *The HIPAA Omnibus Rule: A Compliance Guide for Covered Entities and Business Associates*, *The HIPAA Omnibus Rule Toolkit: A Covered Entity and Business Associate Guide to Privacy and Security*, *h-mail: HIPAA and HITECH Privacy and Security Training Reminders for Healthcare Staff,* and *The No-Hassle Guide to HIPAA Policies: A Privacy and Security Toolkit,* all published by HCPro. She is also the author of 11 specialized HIPAA training handbooks for behavioral health staff; business associates; coders, billers, and health information management 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; and registration and front office staff, also 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.

# Introduction

## HITECH Act and Omnibus Rule Impact on Security

Legislation enacted in 2009 and an expansive rule implemented in 2013 have significantly affected the Health Insurance Portability and Accountability Act (HIPAA). The first is the Health Information Technology for Economic and Clinical Health (HITECH) Act. The second is 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; Other Modifications to the HIPAA Rules, Final Rule, commonly referred to as the Omnibus Rule.

### *The HITECH Act*

The HITECH Act, a subset of the American Recovery and Reinvestment Act of 2009, is of major significance to the healthcare industry because it does the following:

- Provides financial incentives for certain healthcare providers to adopt and use electronic health records (EHR) in a meaningful way that improves patient care
- Strengthens protections for individually identifiable health information

The HITECH Act does not overhaul HIPAA's Security Rule, but all organizations that must comply with this rule (i.e., all covered entities and business associates [BA]) should understand how this law and federal regulations affect them and their information security programs.

### *The Omnibus Rule*

The Omnibus Rule is referred to as such because it incorporates a wide range of changes that affect four other HIPAA rules in the Code of Federal Regulations (CFR) Parts 160 and 164:

- Privacy Rule
- Security Rule
- Breach Notification Rule
- Enforcement Rule

It implements some provisions of the HITECH Act, the Genetic Information Nondiscrimination Act (GINA) of 2008, and additional privacy protections and enhancements required by the U.S. Department of Health and Human Services (HHS). The enforcement date for most Omnibus Rule provisions was September 23, 2013.

### *Meaningful use*

Eligible healthcare providers and hospitals must do the following to receive incentive payments from Medicare and Medicaid programs and to avoid financial penalties in the future:

- Implement EHR systems that have been certified by a government-approved organization
- Use these EHRs in meaningful ways that improve patient care

HHS developed criteria that healthcare providers and hospitals must meet to demonstrate that they are using EHRs effectively for patient care. In turn, HHS developed functional criteria for certified EHRs to ensure that vendors design computer systems that are able to capture these required measurements.

The main focus of meaningful use measures is delivering better healthcare, but HHS also specified various security measures. Certified EHRs must include important technical security features, such as encryption and integrity checking. Providers that seek incentive payments based on their use of EHRs must attest that they have performed a security risk assessment and mitigated risks.

HHS reminds organizations that they already should be performing risk assessments and mitigating risks to comply with the HIPAA Security Rule in force since 2005, so this assessment should not be unexpected. Refer to 45 CFR 164.308(a)(1) [Risk analysis].

When HHS released meaningful use stage 2 criteria, it added language emphasizing that risk assessments must consider the use of encryption. HHS specifically did not intend to modify the Security Rule or impose any new requirement regarding encryption. However, it noted that many reported breaches of

protected health information (PHI) involved lost or stolen devices. If these devices or the PHI had been encrypted in accordance with the Security Rule, these events would not have been breaches. Refer to 45 CFR 164.312(a)(1) [Encryption and decryption].

Hence, all organizations subject to the HIPAA Security Rule should take heed and ensure that they use encryption whenever reasonable and appropriate to do so, not only on portable computing devices and media but also in transmission over the Internet, wireless networks, and where warranted. Refer to 45 CFR 164.312(e)(1) [Encryption]. Otherwise, organizations are required to implement, and document, equivalent alternative measures, because encryption of PHI at rest and in transit are addressable implementation specifications.

### *Privacy protections*

The HITECH Act and the 2013 Omnibus Rule strengthen privacy protections in many ways. The definition of PHI is expanded to include genetic information of individuals and their family members. Individuals have enhanced rights with respect to access to their PHI, receiving electronic copies of their PHI, and restricting disclosure of PHI to health plans when they make full payment for services out of pocket.

Covered entities and BAs are more limited with respect to use and disclosure of PHI for healthcare operations, marketing, and sale. Certain covered entities may use and disclose more PHI for fundraising purposes than was allowed previously, but they also must provide easy opt-out and must strictly honor opt-out requests.

These changes and others, along with breach notification requirements, are deemed material, meaning that covered entities must revise their HIPAA Notices of Privacy Practices.

### *Enforcement*

The HITECH Act led to an interim final Enforcement Rule that the Omnibus Rule has largely adopted as a final rule. Key provisions include extending enforcement authority to state attorneys general and requiring that HHS do more with respect to investigations and compliance audits of covered entities and BAs.

Perhaps most notable is the change in civil penalties for noncompliance with HIPAA rules. The monetary penalties are now tiered based on factors such as willful neglect, and the penalty amounts are significantly higher. Fines at the lowest tier that do not involve reasonable cause or willful neglect can be $50,000 for a single violation or $1.5 million for multiple violations of an identical provision in one calendar year.

## HIPAA/HITECH ACT ADMINISTRATIVE SIMPLIFICATION PENALTIES

**Civil penalties for failure to comply with Privacy, Security, Breach Notification, and other HIPAA Administrative Simplification Rules**

| Violation Tier | Monetary Penalty |
|---|---|
| a. Person did not know (and by exercising reasonable diligence[1] would not have known) that a provision was violated | $100–$50,000 for each violation<br>Up to $1,500,000 for all such violations of an identical provision in a calendar year |
| b. Violation due to reasonable cause[2] and not to willful neglect[3] | $1,000–$50,000 for each violation<br>Up to $1,500,000 for all such violations of an identical provision in a calendar year |
| c. Violation due to willful neglect but corrected within 30 days of knowing, or date when entity exercising due diligence would have known, of the violation | $10,000–$50,000 for each violation<br>Up to $1,500,000 for all such violations of an identical provision in a calendar year |
| d. Violation due to willful neglect and not corrected within 30 days of knowing, or date when entity exercising due diligence would have known, of the violation | $50,000 for each violation<br>$1,500,000 for all such violations of an identical provision in a calendar year |

45 CFR 160.401 definitions:

[1] "*Reasonable diligence* means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."

[2] "*Reasonable cause* means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect."

[3] "*Willful neglect* means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated."

### *Breach notification*

The HITECH Act requires reporting PHI breaches to affected individuals and HHS. Most states have breach notification laws, but they are not uniform, and this is the first federal law that requires breach notification. An interim final Breach Notification Rule was published in 2009. HHS dissatisfaction with covered entity response inspired changes in the Omnibus Rule that strengthen the definition of a breach and the risk assessment process.

The Omnibus Rule preamble in the *Federal Register*, vol. 78, no. 17, January 25, 2013, Part II (45 CFR Parts 160 and 164), notes that some covered entities interpreted the interim rule threshold for reporting breaches higher than HHS intended. Hence, the final Breach Notification Rule within the Omnibus Rule defines a privacy or security incident involving unsecured PHI as a *presumptive breach* unless and until shown otherwise.

Second, covered entities and BAs must conduct a risk assessment to determine the probability that PHI was compromised. Then, unless the risk is determined to be low, the incident or violation is deemed a breach. In cases of obvious breaches, the risk assessment may be omitted and the breach notification process begun. Note that the risk assessment no longer focuses on harm to individuals but risk to the data (i.e., the PHI). The latter is more consistent with traditional security risk assessment processes.

Further, any risk assessment must consider at least four factors that the rule now incorporates. They were in the interim rule preamble but apparently were overlooked by many organizations. The rule at 45 CFR 164.402 [Definitions] includes the following factors:

> *(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;*
>
> *(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;*
>
> *(iii) Whether the protected health information was actually acquired or viewed; and*
>
> *(iv) The extent to which the risk to the protected health information has been mitigated.*

With respect to the HIPAA Security Rule, organizations should thoroughly review and revise their incident response plans and procedures [45 CFR 164.308(a)(6) Security incident procedures] in light of the breach notification changes. Refer to 45 CFR 164.308(a)(6) [Administrative safeguards]. These changes affect

decision trees used to determine whether a PHI breach has occurred. The Omnibus Rule also requires that organizations document the risk assessment and all notifications to demonstrate their compliance.

### *Business associates*

HIPAA compliance enforcement was originally limited to covered entities. The HITECH Act declares that HIPAA-defined BAs are also directly liable for compliance with the HIPAA Security Rule and with relevant provisions of the Privacy Rule.

The Omnibus Rule implements this change, making BAs directly liable to HHS and requiring them to comply with all Security Rule provisions and certain Privacy and Breach Notification Rule provisions. This does not replace BAs' ongoing contractual liability.

The Omnibus Rule clarifies the definition of BA, explicitly including organizations identified in the HITECH Act (e.g., health information organizations, e-prescribing gateways, patient safety organizations, and some personal health record vendors). The rule requires determining whether a person or organization is a BA on a case-by-case basis. The rule preamble that appears in the January 25, 2013, *Federal Register* indicates that certain information technology companies that house PHI and are more than conduits are BAs even if they do not access the data.

Finally, the Omnibus Rule goes beyond the HITECH Act and revises the definition of BA to include all downstream subcontractors with access to PHI. This closes a major loophole in privacy protection. Along with the clarifications discussed previously, the rule significantly expands the number of organizations deemed BAs and directly subject to HIPAA compliance and enforcement.

The rule revises some required language in BA contracts. Refer to 45 CFR 164.308(b)(1) [Administrative safeguards] and 45 CFR 164.314(a)(1) [Organizational requirements]. Covered entities and their BAs must use this language in their contracts; BAs similarly must use this language in their contracts with subcontractor BAs. HHS offers sample language on its website. Most BA contracts or approved alternatives such as memoranda of understanding (MOU) between government agencies require revision and re-signing to incorporate Omnibus Rule changes.

### *Security Rule technical changes*

The Omnibus Rule revises the definition of electronic media to modernize it and align it with National Institute of Standards and Technology (NIST) terminology. For example, the definition previously used the term *electronic storage media* to describe physical devices such as hard drives, magnetic tapes, and USB

(universal serial bus) drives. The revised definition uses the term *electronic storage material* to encompass new storage technologies and trends. The new definition at 45 CFR 160.103 [Definitions] is as follows:

> *Electronic media means:*
>
> *(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;*
>
> *(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.*

This definition continues to exclude, for example, paper documents that are faxed. However, the Privacy Rule protects such documents when they contain PHI.

The term *electronic media* is central to understanding and complying with Security Rule standard 45 CFR 164.310(d)(1) [Device and media controls] and its four implementation specifications (i.e., disposal, media reuse, accountability, and data backup and storage). Covered entities and BAs should ensure that their security policies, procedures, and other controls reflect the full scope of this definition.

The intent of other Security Rule changes effected by the Omnibus Rule is either to more clearly and accurately explain the Security Rule standards' intent or to conform to other changes effected by the Omnibus Rule.

Technical revisions affecting 45 CFR 164.306(e) clarify that covered entities and BAs must have dynamic ongoing programs to protect electronic PHI, including regular updating of security documentation. Security is not a one-time project.

A technical revision in 45 CFR 164.308(a)(3)(ii)(C) is to ensure that termination procedures apply not only to employees but to all workforce members. In practice, procedures also should include access termination of third parties with access to an organization's PHI.

The Omnibus Rule makes numerous technical and conforming changes to 45 CFR 164.308(b) [Business associate contracts and other arrangements] due to the changes regarding the revised BA definition and BAs' new direct liability. It removes certain exceptions to the definition of BA because the definition is beyond the scope of the Security Rule. It streamlines contract and agreement requirements to eliminate duplication with the Privacy Rule's parallel requirements.

Most important, it makes clear that the responsibilities between covered entities, BAs, and their BA subcontractors are link by link. That is, covered entities have responsibility only for their direct BAs, not for their BAs' subcontractors. Each subcontractor BA that further subcontracts PHI-related work is responsible for obtaining a BA contract with its subcontractor(s). Conversely, if a breach of PHI occurs at a subcontractor's subcontractor, the breach reporting must go up the chain, one link at a time; that is, the subcontractor suffering the breach must notify the BA with which it signed a BA contract, who, in turn, notifies the entity with which it signed a BA contract, and so on, up to the affected covered entities.

All covered entities and BAs should ensure that they are referencing and relying on the most current version of the HIPAA Security Rule available at *www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=5f6622f63f427905bc5022cbcfd36dc3&tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl*.

## Conclusion

All covered entities and BAs are required to fully comply with the HIPAA Security Rule. Since the Breach Notification Rule became effective, HHS has received and continues to receive reports of breaches affecting many millions of patients and health plan members. Many of these breaches would not have occurred if more and stronger security measures had been implemented and enforced.

Remember that without security there is no privacy.

*Editor's note: Access the Electronic Code of Federal Regulations at* www.ecfr.gov/cgi-bin/ECFR?SID=2819d30d81ced53a03f5555703ecd405&page=browse.

*Access the Federal Register, vol. 78, no. 17, January 25, 2013, Part II (45 CFR Parts 160 and 164 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; Final Rule) at* www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

CHAPTER 1

# HIPAA Security Introduction and Overview

## What Is HIPAA?

When Congress approved the Health Insurance Portability and Accountability Act of 1996 (HIPAA), it included a major section titled Administrative Simplification. This section requires the healthcare industry to streamline and simplify computer processing of electronic transactions, primarily between providers and payers, such as claims, eligibility checking, and payments. Administrative Simplification mandates standardized record formats and code sets for these transactions. This will result in less customized processing for each different payer and, thus, lower processing and software support costs to the industry. It should also lead to faster turnaround time on claims submission and payment.

Congress anticipated that in the future the healthcare industry will process most, if not all, of these transactions electronically instead of on paper. As the healthcare industry's external business transactions become increasingly electronic, the risks to patient privacy and the security of the information also increase. Hence, Congress included in Administrative Simplification two new regulations to protect these data.

Administrative Simplification directed the U.S. Department of Health and Human Services (HHS) to develop a privacy rule and a security rule. The Privacy Rule became an enforceable regulation as of April 14, 2003. HHS released a final Security Rule in February 2003. However, as with the Privacy Rule, organizations subject to the rule (covered entities) had 24 months, or until April 20, 2005, to prepare before this rule became enforceable. Small health plans with annual revenue less than $5 million had until April 20, 2006, to prepare.

Administrative Simplification defines covered entities as all health plans, healthcare clearinghouses, and those healthcare providers that engage in electronic transactions. The definition generally omits providers that do not submit insurance claims or that submit all claims on paper—typically, only nontraditional or very small provider organizations. If you need help determining whether your organization is a covered

entity, visit the HHS Centers for Medicare & Medicaid Services (CMS) website (*www.cms.gov*) and enter the term covered entity in the search window to access its decision support tool. This self-test helps determine whether an organization is a covered entity.

## How Security Fits In

Privacy and security are closely intertwined. Information privacy addresses each individual's right to control his or her information. Privacy laws describe the conditions under which organizations may use personal information and the obligations of organizations to protect the data. HIPAA's Privacy Rule specifies when an entity may use protected health information (PHI)—essentially any information about a patient or plan member that can be used to identify that individual—with and without the individual's permission.

Information security is the assurance of confidentiality, integrity, and availability of protected information. Confidentiality means that only authorized individuals, with a legitimate business need, have access to PHI. Integrity means that the PHI can be trusted and that it has not been inappropriately altered or destroyed. And availability means that authorized individuals or computer processes can access PHI when they need to do so.

HIPAA's Privacy Rule requires that organizations protect PHI in all forms—oral, written, and electronic—by using administrative, physical, and technical safeguards to ensure confidentiality, integrity, and availability.

However, the Security Rule applies only to electronic PHI (ePHI; i.e., a subset of the PHI that is specifically protected under both the original HIPAA law and the Privacy Rule). This is because the impetus for this rule came from the Administrative Simplification focus on electronic transactions. Nevertheless, it is good business practice for organizations to protect all forms of PHI and other confidential information.

Information security and organizations' security programs constantly change as new risks arise, as business practices evolve, and as HHS modifies its baseline standards. The government reserves the right to make annual changes once rules are in force, and security experts expect the rules will change in the years ahead. Organizations must recognize the importance of security and understand that this is not a one-time compliance project. Security will continue to evolve. Therefore, covered entities and business associates (BA) should view their security efforts in that light and not as a race to the finish line.

HHS has stated that it will not be an accrediting body, nor does it intend to routinely review all covered entities' and BA's compliance. However, HHS will conduct random compliance audits, and if a complaint is filed with HHS, an investigation will occur. In either scenario, HHS may assess penalties. Administrative Simplification provides both civil and criminal penalties. The civil penalties are for noncompliance with the rules. The criminal penalties are broadly for "wrongful disclosure" of PHI, with increasing fines and prison time, depending on the intent behind the wrongful disclosure. Security Rule and Privacy Rule enforcement occur within HHS's Office for Civil Rights. The 2013 HIPAA Omnibus Rule includes the final Enforcement Rule with significantly raised civil penalties for noncompliance.

Covered entities must impose contractual limits and obligations on their BAs as described in Chapter 3. BAs are third parties with access to a covered entity's PHI and who are performing work on behalf of a covered entity or its BA. In addition, note that under the 2013 HIPAA Omnibus Rule, BAs are also directly liable to HHS for compliance with the Security Rule.

## HOW TO MEASURE YOUR ORGANIZATION FOR SECURITY

The terms *small, midsize,* and *large* are used to characterize healthcare organizations throughout this book. The following descriptions will help you place your organization into one of these size categories.

HIPAA does not specifically use these terms, but it does allow flexibility in the way organizations comply with various parts of the rule.

These terms are used to help you determine what compliance activities might be appropriate for your facility. These are intended only as guidelines. You should make your own decisions about your compliance activities based upon your own risk assessment. These descriptions may also guide BAs.

**Small**

Organizations are characterized by:

- A single physical facility
- A single primary software application vendor (excluding desktop software such as Microsoft Office)
- A limited local network, single-platform LAN, with basic access to the Internet (e.g., for transmitting billing files)

***Example:*** *Small office of physicians or dentists*

## HOW TO MEASURE YOUR ORGANIZATION FOR SECURITY (CONT.)

**Midsize**

Organizations are characterized by:

- One primary facility, additional smaller or limited outlying facilities or field operations
- 24/7 operations (or at least having some inpatient care areas)
- Multiple application software vendors, with a small number of "primary" applications and vendors
- Centrally controlled network with multiple platforms (often hosted remotely with the vendor or other third party), Internet connectivity, support for remote access inbound

***Example:*** *Community hospital with 200 beds, outpatient clinics in vicinity, limited home health services*

**Large**

Organizations are characterized by:

- Multiple major facilities, sometimes in more than one state
- 24/7 operations
- Hundreds of applications
- Large and highly complex electronic network (often controlled by multiple groups) with numerous platforms and many thousands of nodes; multiple points of remote inbound and outbound access

***Example:*** *Integrated healthcare delivery system in multiple states with full range of inpatient and outpatient services, plus a health plan*

## How to Use This Book

This book explains the Security Rule in detail and provides practical guidance to organizations for compliance with the rule.

The rule comprises *standards* and *implementation specifications*, terms that are defined in more detail in Chapter 2. Throughout the book, standards are clearly identified with the rule's exact language and with the rule's section reference. Each implementation specification underlying a standard is also presented with the rule's language. Each standard and specification is followed by a discussion of its background and intent, along with practical tips for compliance. The background and intent are derived from the rule's preamble* and, in some cases, from the proposed Security Rule of 1998 and other supporting documents.

### *Compliance step 1: Understand the Security Rule*

In gaining a thorough understanding of the rule and its implications for your organization, you will take an important first step toward compliance. Note that the rule does not specify how an organization should meet each requirement. Because healthcare organizations vary widely in size, complexity, technologies, and resources, the rule provides wide latitude and flexibility for compliance. This makes compliance easier in one sense, but it also means that organizations have significant responsibility for understanding and living up to the intent of the rule. For organizations just getting started with security, there are no simple, black-and-white answers.

### *Compliance step 2: Appoint an information security officer*

You must appoint an information security officer (ISO) who will take the lead in establishing the program and will have ongoing responsibility for it. If you have not yet established a security program, reading this book in its entirety beforehand can help you fully appreciate the scope and skills necessary for this critical role. Establishing such a program requires project management skills and a technical background, but the position entails far more than projects and technology. In all but the smallest organizations, the job is likely to require daily management and strategic planning activities that are far more intensive than the typical privacy officer's role. Chapter 3 includes further discussion of this role.

*The rule's preamble referenced throughout this book appears in the *Federal Register*, vol. 68, no. 34, February 20, 2003, pp. 8376–8377. Access the preamble at *www.cms.gov/Regulations-and-Guidance/Regulations-and-Policies/QuarterlyProviderUpdates/downloads/cms0049f.pdf.*

### *Compliance step 3: Risk assessment*

Once the ISO is designated, and this individual is well versed in the Security Rule, this individual should begin the process of assessing your organization's current risk. The rule requires that each organization evaluate its own particular risks and takes steps to mitigate them.

Whether your organization intends to set the gold standard for your peers or expects a challenge with respect to meeting even the basic requirements, you must understand your risk. The two types of risk are as follows:

- Risk of noncompliance with HIPAA regulations and other laws (e.g., state breach notification laws)
- Security risks to confidentiality, availability, or integrity of information

Generally, if your organization is in compliance with regulations, it is expected to continually address security risk. Remember that, even though your organization may be compliant, this does not mean that it has eliminated all risk. Risk is dynamic, and there is always some risk to your information. Thus, organizations should implement mechanisms to monitor their risk. Both the rule and good security principles require that organizations establish dynamic processes that prevent, detect, contain, and correct security breaches.

After reading this book, you may worry that the work is overwhelming. However, a comprehensive risk assessment, which the rule requires, will provide an overview of your situation and will indicate which risks are a high priority, as well as which risks can be addressed easily and promptly. This assessment creates a blueprint for compliance and sets the stage for project planning, resource allocation, and budgeting steps. Chapter 3 includes more information about the assessment process.

The assessment and project planning phase will set you on the road to compliance. By initiating security planning and addressing high risks now, your organization will be less likely to experience a security breach, and it will be in a more advantageous position in a legal challenge.

Some risks require technical solutions that are not readily available to your organization at this time. These might be risks that you mitigate with compensating controls until you can address them in a more robust manner. For example, projects involving complex technologies that require a long lead time,

significant planning, and new financial and human resources (e.g., evaluating products, negotiating contracts, integrating with existing network and systems, testing, training, and support) may not come to fruition for several years. HHS may consider this if you have identified the risk in your assessment and have a plan to mitigate it.

**FIGURE 1.1 | Quick Start to Compliance**

Small organizations typically designate a single individual to become "security smart." Mid-size and large organizations generally appoint more than one individual, even a team, to become very knowledgeable about security and to implement HIPAA's Security Rule and other security regulations. The job is bigger in a large organization, and such an organization is likely to appoint specialists who can devote more time to security than their counterparts in a small organization.

The following steps are intended as one approach to becoming compliant. Note, however, that these steps are not comprehensive. Security is not a project or a product, it is a process. And an information security program—as required by HIPAA and other laws—is an ongoing, dynamic process without an endpoint.

***Compliance step 1: Understand the Security Rule***

Take time to read the rule, and seek out additional resources such as books, conferences, and seminars about healthcare information security.

***Compliance step 2: Appoint an information security officer***

Develop the job description and consider where to place the new role in your organization. Decide whether to appoint from within or to seek a security professional from outside. Select the individual. Announce the appointment.

***Compliance step 3: Risk assessment and compliance review***

Determine whether internal resources are equipped to perform a reliable assessment, or whether you will rely on outside professionals. Define the methodology and deliverables. Perform the comprehensive assessment. Review identified risks and recommendations. Formally accept lesser risks and develop action plans to mitigate more significant ones. Verify that each Security Rule requirement is already met or will be met upon completion of the mitigation action plans.

## Layered Approach

Risk is a matter of degree, and solutions are generally layered. Normally, you will not eliminate risk; you will mitigate it through multiple mechanisms. Some of these may be technical, some may be physical, and some may be administrative (e.g., workforce training and procedures).

The following approach to the fundamental security concept of access control represents an example of layered solutions. You must control access to PHI to reasonably ensure that only authorized individuals have access to it. Note that access control is relative, not absolute. Even if you take reasonable measures, there may still be a way for someone to "break in" and gain access. In an electronic environment, this goal typically is achieved through a variety of administrative, physical, and technical mechanisms that might include the following elements:

- Use of firewalls
- Adherence to server configuration standards
- Adoption and use of change control procedures
- Locked data centers and server rooms
- User authorization procedures
- Workforce training about password management

Using this layered approach, you can emphasize certain controls to compensate for others that are deficient to provide a reasonable and appropriate level of security. For example, if your vendor application-level security features are weak, you may decide to compensate by more fully employing operating system level controls and providing enhanced user training.

## Some Pitfalls to Avoid

Once your organization learns what the Security Rule requires, your ISO is leading the security program, and your security program is under way, be aware of the following common pitfalls:

- Avoid the urge to immediately solve known security problems. Wait until you have a complete assessment and you see the full picture. You may decide that other security issues are more urgent and deserve a higher priority based on staff or budget resources. Or you may find that solutions are interdependent. By prematurely applying a technical solution to one problem, you may have complicated or worsened other security flaws, or you may have missed an opportunity for an integrated solution. As with any project, and especially one this big, be sure to take time to plan before acting.

- Avoid focusing primarily or exclusively on technology. Actually, much if not most of security is administrative work: policies, standards, procedures, and training.

- Avoid letting technology dictate policy. Ideally, establish policy first with available technology solutions in mind and then implement the supporting procedures and technologies to fit the policy.

- Avoid buying the wrong technology or too much technology. Sometimes vendor "hype" and technical gadgetry create a strong pull. Ensure that you understand the problem to be solved and thoroughly investigate impact and options before investing in new security technologies. Any technology you select should be the best solution for your particular problem in your risk environment, keeping in mind your resources.

- Avoid underestimating the human resources and skills necessary to achieve reasonable security. Two very common problems in healthcare today are lack of security expertise and understaffing of security-related information technology (IT) roles.

Notice that most of the previous suggestions tend to rein in technology spending. Healthcare organizations on a tight budget can often achieve reasonable security without the latest technology. This is because administrative controls such as following procedures and providing workforce training are largely technology independent, core security technologies are usually not expensive, and savvy IT staff can sometimes use freeware or shareware instead of buying vendor proprietary products. Vendor products generally have easier-to-use interfaces and more articulate reporting, but they sometimes

perform the same functions as freeware. Be aware, however, of the efficiencies that user-friendly commercial products may offer over freeware. Making effective use of freeware requires time and skill that may cost more than purchasing a commercial solution.

## Documentation Tips

Finally, remember the following general policy and procedure compliance tips:

- Organizations sometimes neglect to document policies and procedures. The rule requires it, but there is also true value to documentation. First, documentation forces you to review your processes. This helps you uncover gaps and inconsistencies, enabling you to design new solutions or protective countermeasures. Second, documentation helps ensure that everyone understands the organization's expectations. Third, it also helps ensure consistency (i.e., everyone performs the same process in the same manner). Finally, clear and current policies and procedures provide an invaluable training tool for new workforce members.

- If you work for a small organization, remember that HIPAA allows you to write standard operating procedures instead of formal policies. These documents are typically brief and combine a policy goal with specific procedures. What is important is the content and the fact that the policy is documented and followed by your workforce.

- Larger, more complex organizations should separate policies from procedures. This allows implementing different procedures in different parts of an organization, all in support of the same policy. Also, policies should be fairly high level and relatively stable to withstand the test of time with periodic (e.g., annual) review. They should not include specific technologies or technical standards, because these are the solutions that implement the policy and may vary. Conversely, standards and procedures must be detailed, and they should be relatively easy to change (i.e., not require an organizationwide review process as policies do). Policies are global; procedures are local.

  – For example, a policy may state that access to confidential information including PHI requires prior documented authorization. Underlying procedures may include maintenance of access authorization lists, access request forms, procedures for completing and submitting request forms, setting up computer access, Access to different systems may occur via different forms and procedures. For example, registration system request forms must be

sent to John Dow at extension 4321, while billing system request forms must be sent to Mary Ortega at extension 6543.

- When the rule requires a policy, write a policy (or incorporate language into an existing one) that paraphrases the rule. For example, the following policy statement incorporates rule language that satisfies the policy requirement of the contingency plan standard and its underlying specifications:

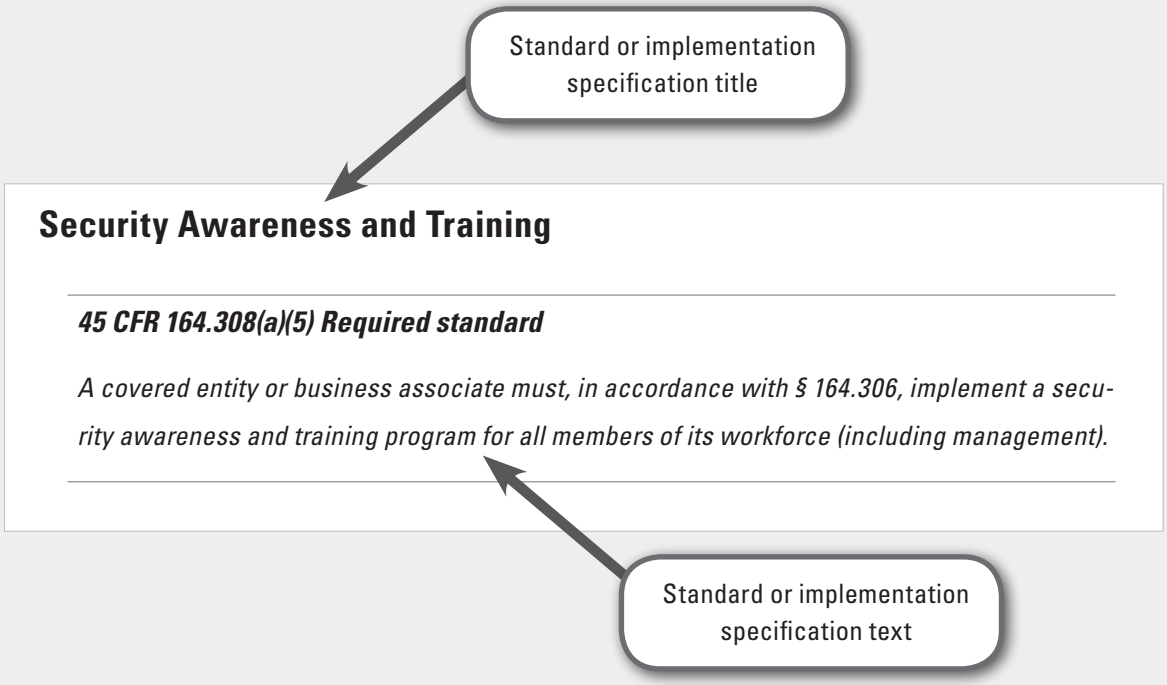
  *This organization shall have an overall contingency plan and supporting procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information and other confidential and proprietary data. This plan will include procedures for data backup, procedures for periodic system criticality analysis, a disaster recovery plan, an emergency mode operation plan, and procedures for testing and revision of such plans.*

- Information security is generic. Avoid writing policies applicable to PHI only. Instead, information security policies should protect all confidential information assets. Your organization is likely subject to additional laws and industry standards that require protection of other information (e.g., employee Social Security numbers).

Following these suggestions will make policy writing more straightforward. Carefully considered, well-written policies form the foundation of your information security program, so it is worth the time to get it right.

## A NOTE ABOUT THE FORMAT OF THIS BOOK

*HIPAA Security Made Simple* mirrors the structure of the HIPAA Security Rule. Each chapter consists of sections, and each section is identified by the standard or its underlying implementation specification that is the subject of that section. The actual standard or implementation specification language is highlighted in bold at the beginning of each section. A tab at the edge of each page identifies the standard or implementation specification associated with that page.



SECOND EDITION

# HIPAA SECURITY MADE SIMPLE

## Practical Compliance Advice for Covered Entities and Business Associates

**Kate Borten, CISSP, CISM**

Written by highly respected author Kate Borten, CISSP, CISM, this updated edition explains how the Omnibus Rule affects organizations that are subject to HIPAA. It will help facilities and business associates (BA) understand how they and their information security programs can remain in compliance with new and existing regulatory requirements.

This second edition emphasizes that security is not a one-time project and reminds readers that they should already be performing risk assessments to comply with the HIPAA Security Rule. A new Introduction explains the significance of the HITECH Act and the Omnibus Rule to covered entities and their BAs. HITECH made BAs directly liable for Security Rule compliance, and the Omnibus Rule went further, revising the definition to include all downstream subcontractors with access to PHI. This closed a major loophole in privacy protection, significantly expanding the number of organizations deemed BAs and directly subject to HIPAA compliance and enforcement.

**This book explains how HIPAA and the Omnibus Rule do the following:**

- Clarify the definition of BA, which now includes all downstream subcontractors with access to PHI
- Clarify that covered entities and BAs must have ongoing programs to protect electronic PHI, including regular updates to security documentation
- Revise and modernize the definition of electronic media to align it with the terminology used by the National Institute of Standards and Technology
- Ensure that access termination procedures apply to all workforce members, not just employees
- Make encryption an addressable implementation specification

HSMS2

HCPro

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

ISBN: 978-1-61569-273-6