HIPAA Security Overview - Retired

Save to myBoK

Editor's note: This update replaces the April 2004 and the November 2010 practice briefs titled "A HIPAA Security Overview."

The HIPAA security rule has remained unchanged since its implementation more than a decade ago. However, the Health Information Technology for Economic and Clinical Health (HITECH) Act, amended by the Omnibus Rule on January 25, 2013, includes provisions that change several important aspects of the rule. The Omnibus Rule requires the compliance of business associates (BAs) and their subcontractors. It also requires the Office for Civil Rights (OCR) to perform audits that include stiffer penalties for non-compliance. Achieving compliance requires organizations to maintain and implement effective written policies and procedures as well as implement safeguards and controls.

The HIPAA Security Rule describes safeguards as the administrative, physical, and technical considerations that an organization must incorporate into its HIPAA security compliance plan. Safeguards include technology, policies and procedures, and sanctions for noncompliance.

This practice brief provides a succinct overview of the security rule, along with some of the background and basic concepts necessary to understand the security rule. In addition, it highlights the skills that health information management (HIM) professionals possess to maintain HIPAA security compliance within their organizations.

Background

The Department of Health and Human Services (HHS) published the HIPAA security rule on February 20, 2003. With the exception of small health plans that had until April 21, 2006 to comply, Covered entities (CEs) should have been in compliance no later than April 21, 2005—two years from the original date of publication. However, even today, CEs have difficulty maintaining and documenting compliance with the security rule's requirements.

Although the HIPAA privacy rule covers all protected health information (PHI) in an organization, the HIPAA security rule is narrower in scope and focuses solely on electronic PHI (ePHI). Section 164.530 of the HIPAA privacy rule requires "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The security rule complements the privacy rule by establishing the baseline for securing ePHI both in transit and at rest.

The HIPAA security rule is based on three principles: comprehensiveness, scalability, and technology neutrality. It addresses all aspects of security, does not require specific technology to achieve effective implementation, and can be implemented effectively by organizations of any type and size.

Basic Concepts

CEs include healthcare plans, healthcare clearinghouses, and healthcare providers that electronically maintain or transmit PHI. As previously stated, the HITECH Act, which is part of the American Recovery and Reinvestment Act (ARRA), and amended by the Omnibus Rule, requires BAs to comply with the HIPAA security rule. This means that BAs are now subject to the same criminal and civil penalties as CEs. The HITECH regulations, which required compliance by September 23, 2013, also include enhanced penalties and a national breach notification requirement. This requirement specifies that in the event of a breach of PHI, organizations must notify the individual(s) to which the PHI is applicable as well as HHS. If the breach affects more than 500 individuals, the organization must also notify the local media.

ePHI includes PHI that is simply maintained (i.e., at rest) or PHI that is transmitted (i.e., in transit). Examples of ePHI at rest include patient information stored on magnetic tapes, optical discs, internal and external hard drives, DVDs, USB thumb drives, smartphones, and storage area networks. ePHI in transit includes patient information sent between computer systems (internal

and external). The security risks are generally greater when ePHI is being transmitted outside of an organization's internal network. This includes sending information via the Internet and extranet technology, leased lines, and private networks. However, security breaches of ePHI in transit can also occur internally by authorized users.

HIPAA security implementation specifications are either required (i.e., must be implemented as stated in the rule) or are addressable (i.e., must be implemented as stated in the rule or in an alternate manner that better meets the organization's needs while still meeting the intent of the implementation specification). Although addressable specifications offer some flexibility to organizations these specifications are still required. Organizations choosing an alternate method of implementation for addressable specifications must maintain formal documentation regarding why and how the specification is implemented.

Information security is the preservation of confidentiality, integrity, and availability of information. In a healthcare setting, this security includes ePHI used for clinical decision making or healthcare operations.

Scalability allows organizations to identify security measures appropriate for its own unique operational risks and other factors. These factors include the organization's size and complexity, hardware and software, costs of implementing additional security, and the threats and vulnerabilities identified during a risk analysis.

The Security Rule at a Glance

The HIPAA security rule standards are grouped into five categories: administrative safeguards; physical safeguards; technical safeguards; organizational standards; and policies, procedures, and documentation requirements. One of the most important steps in preparing to implement these standards is to review the HIPAA security rule itself. The most important elements of the rule are summarized below.

Administrative safeguards (section 164.308) include nine standards:

1. Security management functions. This standard requires organizations to analyze their security risks and implement policies and procedures that prevent, detect, and correct security violations. It also requires organizations to define appropriate sanctions for security violations. Security management is the foundation of the HIPAA security rule. Performing a thorough risk analysis and developing a corresponding risk management plan are an integral first step toward compliance with this standard.
    - Tip: One of the keys to this section is to use risk analysis to prioritize the security management process. Identify the specific controls (i.e. stronger passwords, email encryption, intrusion prevention software, locking down USB ports) that the organization will implement. Ensure enforcement of policies and procedures by applying sanctions and reviewing system activity regularly.
2. Assigning security responsibility (no implementation specifications) requires organizations to identify the individual responsible for overseeing development of the organization's security policies and procedures.
    - Tip: This role must include a job description. Everyone in the organization should be able to identify this individual and his or her role.
3. Workforce security (three implementation specifications) requires organizations to develop and implement policies and procedures to ensure that members of the workforce have access to information appropriate for their job. It also requires organizations to have clear termination procedures.
    - Tip: Workforce extends beyond employees (review HR policies for further clarification) to physicians (Credentialing Office) and contract workers, so a process must be in place to validate, add, and remove users.
4. Information access management (three implementation specifications) requires organizations to implement procedures authorizing access to ePHI.
    - Tip: Document clearly who can authorize the access to PHI for the organization's workforce (i.e., employees, vendors, contractors).

5. Security awareness and training (four implementation specifications) require a security awareness and training program for all members of the workforce, including management.
    - Tip: Although only four areas (security reminders, protection from malicious software, log-in monitoring, and password management) of specific training are mentioned, organizations should train staff on their overall policies and practices to protect the security of ePHI.
6. Security incident procedures (one implementation specification) require that there be policies and procedures for reporting and responding to security incidents.
    - Tip: Refer to the Omnibus Rule to meet compliance with this standard.
7. Contingency planning (five implementation specifications) requires organizations to develop and implement policies and procedures for responding to an emergency or an unusual occurrence (i.e., a fire, vandalism, or natural disaster) that damages equipment or systems containing ePHI, making the information unavailable to caregivers.
    - Tip: Ensure that critical information is available at patients' bedsides. .
8. Evaluation (no implementation specifications) requires a technical and a nontechnical review, including periodic monitoring of adherence to security policies and procedures, documentation of the results of those monitoring activities, and implementation of appropriate improvements in policies and procedures.
    - Tip: The OCR issued the *HIPAA Audit Program Protocol* that can assist organizations in conducting an evaluation. However, the protocol does not address each standard. Organizations must ensure that their evaluation includes all HIPAA, HITECH, and Breach Notification requirements.
9. BA contracts and other arrangements (one implementation specification) requires contracts between CEs and BAs to provide satisfactory assurance that appropriate safeguards will be applied to protect the ePHI that is created, received, maintained, or transmitted on behalf of the CE.
    - Tip: Identify all data that is shared with organization and reconcile this with all business associate agreements (BAAs).

Physical safeguards (section 164.310) include four standards:

1. Facility access controls (four implementation specifications) requires limitations on physical access to equipment and locations that contain or use ePHI.
    - Tip: Ensure physical security over equipment that transmits information, such as wireless and wired networks.
2. Workstation use (no implementation specifications) requires organizations to document the specific tasks that employees can perform at each workstation. It also requires documentation of the manner in which these tasks can be performed as well as the physical attributes of the areas in which workstations with access to ePHI are located.
    - Tip: Some language considerations to consider include only allowing terminals business purpose use only, restricting users from downloading or implementing software (i.e., games, music, movies) and not leaving terminals unattended without logging out of workstation or locking it.
3. Workstation security (no implementation specifications) requires a description of how workstations permitting access to ePHI are protected from unauthorized use. Workstations include mobile devices, such as laptops, tablets, and smart phones.
    - Tip: Workstation security might require encryption for mobile devices, screen savers, automatic logoff and locking down laptops on workstations on wheels (WOWs).
4. Device and media controls (four implementation specifications) require organizations to address the receipt and removal of hardware and electronic media containing ePHI. Organizations must adhere to this standard when using, reusing, and

disposing of electronic media containing ePHI both within and outside the organization.

- Tip: Often times organizations focus on desktop computers and laptops, but electronic media includes CDs, DVDs, computer hard drives, external or portable hard drives, backup tapes, and USB memory devices (i.e., flash drives, thumb drives, jump drives, copier and printer hard drives, bio-medical devices).

Technical safeguards (section 164.312) include five standards:

1. Access control (four implementation specifications) requires controls for limiting access to ePHI to only those persons or software programs requiring the information to do their jobs.
    - Tip: One of the implementation specifications is for the use of encryption and decryption of data at rest. The need for encryption of data at rest (e.g., data on laptops, thumb drives, mobile devices, and databases) is increasingly common and necessary due to the breach notification requirements when unencrypted data is lost or stolen.
2. Audit controls (no implementation specifications) requires installation of hardware, software, or manual mechanisms to examine activity in systems containing ePHI.
    - Tip: This regulation, which requires audit controls, works in collaboration with the information system activity review implementation specification under the security management process standard. The technical capabilities of audit controls must be available in order to review information system activity.
3. Integrity (one implementation specification) requires policies and procedures that protect ePHI from being altered or destroyed in an unauthorized manner.
    - Tip: For application systems, ask the vendor what controls have been implemented (i.e., hash totals) that provide for the integrity of the system.
4. Person or entity authentication (no implementation specifications) requires implementation of measures (i.e., user identification and password) to prevent unauthorized users from accessing ePHI.
    - Tip: Different authentication methods may need to be employed, passwords may be appropriate for internal use, however remote access may require more sophisticated authentication methods (i.e. one-time passwords, VPNs).
5. Transmission security (two implementation specifications) requires mechanisms to protect ePHI that is transmitted electronically from one organization to another.
    - Tip: Encryption of data in transit should be used when deemed appropriate. This certainly includes data in transit over the external internet (i.e., for remote access and email).

Organizational requirements (section 164.314) include two standards:

1. BA contracts or other arrangements (two implementation specifications) require organizations to document that their BA contracts or other arrangements comply with the security measures
    - Tip: As previously noted, because of the HITECH Act, organizations should review and update their BAAs or create addenda to existing BAAs to meet compliance under the final Omnibus Rule.
2. Requirements for group health plans (one implementation specification) require each organization to ensure that its plans complies with appropriate safeguards to protect the security of ePHI. This compliance must be documented.
    - Tip: All activities and resources pertaining to compliance with the HIPAA Regulations must be accurately documented, retained and easily accessible.

Policies, procedures, and documentation requirements (section 164.316) include two standards:

1. Policies and procedures (no implementation specifications) requires that organizations must implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the security rule.

    - Tip: When creating policies, you should address each standard and implementation feature, describe what the organization will do to meet the standard and how this policy will be monitored or compliance with the policy documented.

2. Documentation (one implementation specification) requires organizations to keep written or electronic records of policies and procedures implemented to comply with the security rule. These records must be maintained for six years from the date of creation or the date when last in effect.

    - Tip: Include an effective date on any documentation (policies, procedures, plans, etc.) is useful for meeting HIPAA's requirement for documentation retention. In the event of an audit, it is also important that organizations create and maintain documentation to illustrate that the organization is following its policies and procedures. Such documentation could include incident investigation reports, sanctions, and training documents. When possible, include this monitoring/reporting requirement in all security policies. Ensure that the documentation can be retrieved quickly in the event of an audit and as needed to those persons responsible for implementing the policies. They should also be easily accessible to all workforce members such as by placing them on an Intranet site, making the manuals accessible to user departments, etc..

References

Amatayakul, Margret, et al. "Handbook for HIPAA Security Implementation." American Medical Association, October 2003.

Gallagher, Lisa, Herzig, Terrell. Walsh, Tom. "Implementing Information Security in Healthcare: Building a Security Program" presented at HIMSS, 2013.

Department of Health and Human Services. "Health Insurance Reform: Security Standards; Final Rule." *Federal Register* 68, no. 34 (Feb. 20, 2003). Available online at http://edocket.access.gpo.gov/2003/pdf/03-3877.pdf.

Department of Health and Human Services. "Security Rule Guidance Material." Available online at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.

Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health Information; Final Rule." *Federal Register* 67, no. 157 (Aug. 14, 2002). Available online at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-20554-filed.pdf.

Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of the American Recovery and Reinvestment Act (Public Law 111-5), enactment on February 17, 2009.

"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." 45 CFR Parts 160 and 164. *Federal Register* 78, no.17 (January 25, 2013)

National Institute of Standards and Technology. "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." *NIST Special Publication* 800-66, Revision 1. October 2008. Available online at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

National Institute of Standards and Technology. "Guide for Conducting Risk Assessments" *NIST Special Publication* 800-30, Revision 1. September 2012. Available online at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

OCR. "HIPAA Audit Program Protocol" available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

Prepared by

William Miaoulis, CISA, CISM

Assisted by

Tom Walsh, CISSP

Acknowledgments

Katherine Andersen, RHIT, CCS
Marlisa Coloso, RHIA, CCS
Kathy Downing, MA, RHIA, CHPS, PMP
Kim Turtle Dudgeon, RHIT, CHTS-IS/TS, CMT
Elisa R Gorton, RHIA, CHPS, MAHSM
Judi Hofman, BCRT, CHPS, CAP, CHP, CHSS
Sandra L. Joe, MJ, RHIA
Lesley Kadlec, MA, RHIA
Kelly McLendon, RHIA, CHPS
Nancy Prade, MBA, RHIA, CHPS
Patti Reisinger, RHIT, CCS
Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA
Diana Warner, MS, RHIA, CHPS, FAHIMA

Prepared by (2010)

William Miaoulis, CISA, CISM

Acknowledgments (2010)

Tom Walsh, CISSP

Prepared by (original)

Carol Ann Quinsey, RHIA, CHPS, AHIMA professional practice manager

Acknowledgments (original)

Assistance from the following individuals is gratefully acknowledged:

AHIMA Professional Practice Team
Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS
Gwen Hughes, RHIA, CHP
Kelly McLendon, RHIA
Tom Walsh, CISSP

Article citation:
AHIMA Practice Brief. "HIPAA Security Overview - Retired" (Updated November 2013)

Driving the Power of Knowledge