HIPAA Security Overview (2010 update)

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Editor's note: This update replaces the April 2004 practice brief "A HIPAA Security Overview."

A great deal has been published about the HIPAA security rule in the past. Provisions in the Health Information Technology for Economic and Clinical Health (HITECH) Act include higher noncompliance penalties, breach notification requirements, and the increased likelihood of audits. The HITECH Act has also increased the pressure on organizations to become HIPAA compliant.

This practice brief will provide a succinct overview of the security rule, along with some of the background and basic concepts needed to understand it. In addition, it will outline some of the skills HIM professionals possess that may aid in maintaining compliance with the security rule in their organizations. There is also a list of resources, including guidelines issued by the Department of Health and Human Services (HHS) that may be useful in furthering your knowledge about this subject.

Background

HHS published the HIPAA security regulations on February 20, 2003. As with the HIPAA privacy rule, covered entities had two years from the publication date to comply. Most covered entities should have been in compliance no later than April 21, 2005. (Small health plans had until April 21, 2006, to comply.) Covered entities have had difficulty documenting compliance with the security rule's requirements. To be fully compliant, an organization must have written and up-to-date policies and procedures, maintain compliance with those policies and procedures, and, most importantly, be able to demonstrate (monitor) overall compliance.

Although the privacy rule covers all protected health information (PHI) in an organization, the security rule is narrower in scope, with the focus solely on electronic PHI (EPHI). Section 164.530 of the 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 electronic health information for covered entities both in transit and at rest.

The 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.[1]

Basic Concepts

Covered entities include healthcare plans, healthcare clearinghouses, and healthcare providers who electronically maintain or transmit PHI. The HITECH Act, which is part of the American Recovery and Reinvestment Act, requires business associates (BAs) to comply with the HIPAA security rule. BAs are now subject to the same criminal and civil penalties as covered entities (section 13401 of the HITECH Act). The HITECH regulations also include enhanced penalties and a national breach notification requirement that requires notification to the individual and to HHS when EPHI has been breached. If the breach affects more than 500 individuals, then local media also must be notified. HITECH has taken HIPAA to more organizations and has enhanced the need for HIPAA compliance.

EPHI is PHI maintained (at rest) or transmitted (in transit) in electronic form. Some examples of EPHI at rest include patient information stored on magnetic tapes, optical discs, hard drives (internal and external), DVDs, USB thumb drives, and servers. EPHI transmission occurs when EPHI is being sent between computer systems. The risks are generally greater when EPHI is being transmitted outside of an organization's internal network, including Internet and extranet technology, leased lines, and

private networks; however, insiders pose significant risks, and study results show that most breaches (confidentiality breaches) are from authorized users.[2]

Implementation specifications provide direction as to how the standards should be executed. All standards must be implemented. However, implementation specifications may be either required or addressable. Required implementation specifications must be implemented. Addressable implementation specifications 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. Addressable implementation offers some flexibility to organizations in implementing the standard; however, the standards are not optional, and all must be addressed. Organizations must maintain formal documentation about why and how the implementation specification in the security rule was implemented in an alternate manner.

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

Safeguards (controls) described in the final rule include administrative, physical, and technical issues an organization must consider in its plans to implement the standards, as well as implementation specifications included in the security rule. Safeguards are not limited to technology; they also require policies and procedures for the workforce to follow and sanctions for noncompliance.

Scalability allows an organization to decide on security measures appropriate to its operational risks. Such factors as the organization's size and complexity, hardware and software, costs of implementing additional security, and the threats and vulnerabilities identified in a risk analysis guide an organization in implementing appropriate measures.

The Security Rule at a Glance

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 the security rule is to read and study the rule itself. The most important elements are summarized below.

Administrative safeguards (section 164.308) include nine standards:

- Security management functions (four implementation specifications) require organizations to analyze their risks to security and implement policies and procedures that prevent, detect, and correct security violations and to define appropriate sanctions for security violations. Security management is the foundation of the HIPAA security rule, and performing a meaningful risk analysis and a corresponding risk management plan are an integral first step.
- Assigning security responsibility (no implementation specifications) requires that organizations identify the individual responsible for overseeing development of the organization's security policies and procedures.
- Workforce security (three implementation specifications) requires organizations develop and implement policies and procedures to ensure that members of the workforce have access to information appropriate for their jobs and have clear termination procedures.
- Information access management (three implementation specifications) requires organizations to implement procedures authorizing access to EPHI.
- Security awareness and training (four implementation specifications) require a security awareness and training program for all members of the workforce, including management.
- Security incident procedures (one implementation specification) require that there be policies and procedures for reporting and responding to security incidents.
- Contingency planning (five implementation specifications) requires an organization develop and implement policies and procedures for responding to an emergency or occurrence (such as fire, vandalism, or natural disaster) that damages equipment or systems containing EPHI such that information is not available to caregivers when and where it is needed.
- Evaluation (no implementation specifications) requires a technical and a nontechnical review, including periodic monitoring of adherence to security policies and procedures, documenting the results of those monitoring activities and making appropriate improvements in policies and procedures.
- BA contracts and other arrangements (one implementation specification) require that contracts between a covered entity and BAs provide satisfactory assurance that appropriate safeguards will be applied to protect the EPHI created,

received, maintained, or transmitted on behalf of the covered entity.

Physical safeguards (section 164.310) include four standards:

- Facility access controls (four implementation specifications) require limitations on physical access to equipment and locations that contain or use EPHI.
- Workstation use (no implementation specifications) requires descriptions of which tasks can be performed at each workstation, the manner in which tasks can be performed, and the physical attributes of areas where workstations with access to EPHI are located.
- Workstation security (no implementation specifications) requires a description of how workstations permitting access to EPHI are protected from unauthorized use, including portable devices such as laptops, tablets, PDAs, and other handheld devices, including some types of cell phones.
- Device and media controls (four implementation specifications) require organizations to address the receipt and removal of hardware and electronic media that contain EPHI, which includes the use, reuse, and disposal of electronic media containing EPHI both within and outside the organization (for example, CDs, DVDs, computer hard drives, external or portable hard drives, backup tapes, and USB memory devices [flash drives, thumb drives, jump drives]).

Technical safeguards (section 164.312) include five standards:

- Access control (four implementation specifications) requires controls for limiting access to EPHI to persons or software programs requiring the EPHI to do their jobs.
- Audit controls (no implementation specifications) require installation of hardware, software, or manual mechanisms to examine activity in systems containing EPHI.
- Integrity (one implementation specification) requires policies and procedures that protect EPHI from being altered or destroyed in an unauthorized manner.
- Person or entity authentication (no implementation specifications) requires implementation of measures to prevent unauthorized users from accessing EPHI (for example, user identification combined with a password).
- Transmission security (two implementation specifications) requires mechanisms to protect EPHI that is being transmitted electronically from one organization to another.

Organizational requirements (section 164.314) include two standards:

- BA contracts or other arrangements (two implementation specifications) require organizations to document that their BA contracts or other arrangements comply with the security measures when handling EPHI. As previously noted, because of the HITECH Act, organizations should review and update their BA agreements or create addenda to existing BA agreements.
- Requirements for group health plans (one implementation specification) require each organization to ensure that its plan documents that appropriate safeguards will be implemented for EPHI.

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

- Policies and procedures (no implementation specifications) state that organizations must implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the security rule.
- Documentation (one implementation specification) requires that written or electronic records of policies and procedures implemented to comply with the security rule be maintained for six years from the date of creation or the date when last in effect.

  Tip: Including an effective date on any documentation (policies, procedures, plans, etc.) is useful for meeting HIPAA's requirement for documentation retention.

Notes

1. Amatayakul, Margret, et al. *Handbook for HIPAA Security Implementation*. Chicago: AMA Press, 2004, p. 8.
2. Finance|Tech News. "What's to Blame for 90% of Data Theft?" March 2009.

References

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.

National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995. Available online at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

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. October 2008. Available online at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

Prepared by

William Miaoulis, CISA, CISM

Acknowledgments

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. "HIPAA Security Overview (2010 update)." (Updated November 2010).
