AHIMA
American Health Information Management Association®

HIM Body of Knowledge
FORE Library

A HIPAA Security Overview (AHIMA Practice Brief)

A great deal has been published about the HIPAA security rule in the past year. 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, the article will outline some of the skills HIM professionals have that may aid in implementing the security rule in their organizations. Also included is a list of resources that may be useful in furthering your knowledge of this subject.

Background

The final HIPAA security regulations were published on February 20, 2003, by the Department of Health and Human Services. As with the HIPAA privacy rule, its roots are found in the Health Insurance Portability and Accountability Act of 1996. As with the privacy rule, covered entities have two years to comply with the security rule. Most covered entities must comply no later than April 21, 2005. (Small health plans have until April 21, 2006, to comply.)

While 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. Section 164.530 of the privacy rule requires "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The final security rule approved in February 2003 complements the privacy rule by establishing the baseline for securing electronic health information for covered entities.

The security rule is based on three principles: comprehensiveness, scalability, and technology neutrality. The rule addresses all aspects of security, ensures that the rule can be implemented effectively by organizations of any type and size, and does not require specific technology to achieve effective implementation.1

Basic Concepts

Covered entities include healthcare plans, healthcare clearinghouses, and healthcare providers who electronically maintain or transmit PHI.

Electronic protected health information (EPHI) is PHI maintained or transmitted in electronic form. The security rule does not distinguish between electronic forms of information. Some examples of EPHI are patient information stored on magnetic tapes or disks, optical disks, hard drives, and servers. Examples of transmission media include Internet and extranet technology, leased lines, private networks, and removable media such as disks.

Some examples of information that would not be covered by the security rule include information not in electronic form before the transmission, messages left on voice mail, or paper-to-paper faxes that were not in electronic form prior to the transmission. For purposes of the security rule, copy machines are not considered electronic.

Implementation specifications provide direction as to how the standards should be executed. All standards must be implemented. However, implementation specifications may be "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. This offers some flexibility to organizations in implementing the standard. Organizations must document why the implementation specification in the security rule was implemented in an alternate manner.

Information security is the preservation of confidentiality, integrity, and availability of electronic patient information used for clinical decision making or healthcare operations. Safeguards are described in the final rule to include administrative, physical, and technical issues an organization must consider in its plans to implement the standards and implementation specifications included in the security rule. Safeguards are not limited to technology; they also require policies and procedures for the work force to follow and sanctions for noncompliance.

Scalability allows an organization to decide on security measures appropriate to its operational risks. Such things 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 you will take in preparing to implement the security rule is to read and study the rule. The most important elements are summarized below.

Administrative safeguards (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. Assigned security responsibility (no implementation specifications) requires that organizations identify the individual responsible for overseeing development of the organization's security policies and procedures.

Work force security (three implementation specifications) requires organizations to have policies and procedures to ensure that members of the work force have access to information appropriate for their jobs and 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 work force, including management.

Security incident procedures (one implementation specification) require that there be policies and procedures for reporting and responding to security incidents. Contingency plan (five implementation specifications) requires an organization to have 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 that organizations periodically monitor adherence to security policies and procedures, document the results of monitoring activities, and make appropriate improvements in policies and procedures.

Business associate contracts and other arrangements (one implementation specification) require that contracts between a covered entity and business associates 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 (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 what 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 workstations such as laptops and PDAs.
Device and media controls (four implementation specifications) require organizations to address the receipt and removal of hardware and electronic media that contain EPHI. This includes the use, reuse, and disposal of electronic media containing EPHI both within and outside the organization (for example, a third-party vendor's potential reuse of back-up tapes).

Technical safeguards (164.312) include five standards:

Access control (four implementation specifications) requires policies and procedures 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 any way.

Person or entity authentication (no implementation specifications) requires implementation of measures to prevent unauthorized users from accessing EPHI.
Transmission security (two implementation specifications) requires mechanisms to protect EPHI that is being transmitted electronically from one organization to another.

Organizational requirements (164.314) include two standards:

Business associate contracts or other arrangements (two implementation specifications) require organizations to document that their business associate contracts or other arrangements comply with the security measures when handling EPHI.

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 (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 a period of six years from the date of creation or the date when last in effect.

HIM Professionals' Skills and Responsibilities

HIM professionals have knowledge and skills that can add value to the planning and implementation of security measures to comply with the HIPAA security rule. These include:

Understanding of federal and state law and accreditation standards as they relate to confidentiality and privacy of PHI in all formats.

Expertise about electronic disclosures that can and should be made versus those that should not

Experience defining appropriate access to PHI based on the needs of the patient, work force, and federal and state laws and regulations

Knowledge of the organization's compliance efforts with the privacy rule

Development of policies, procedures, standards, and Guidelines

Educating the work force relative to privacy- and security-related policies and procedures

Experience measuring effectiveness and compliance with requirements for licensure and accreditation

Design of audit processes and programs

Strong organizational and collaborative skills

Service as privacy or security officers for the organization

HIM professionals are often in a position to foresee the effect of security systems on work flow throughout the organization and can assist in achieving compliance with such systems. Typically, they have strong communication links with members of the executive, nursing, ancillary, and medical staffs, so they can be of great assistance in implementing required work flow changes.

HIM professionals can also make great trainers for privacy and security because of their ability to tie the theory behind the rules to actual practice for those being affected by changes. Their knowledge of various departments' roles in delivering healthcare can help them create realistic examples for staff in multiple departments and can make an enormous contribution to effective training and successful implementation.

Conclusion

The first step in the journey toward implementing security is to read the security rule. The rule is organized in a way that flows logically from conducting a risk analysis through implementing systems, policies, and procedures that allow you to comply with the rule. Many organizations already have excellent information security provisions in place. Nothing in the rule requires costly system changes unless they are deemed appropriate to an organization, nor does the rule require implementing systems that will impair your ability to do business in an efficient and cost-effective way. It seems imminently reasonable to think that the implementation of good security practices could enhance the business of delivering healthcare. The next step is to get involved in your organization's efforts to comply with implementation of the HIPAA security rule.

Note

Amatayakul, Margret et al. Handbook for HIPAA Security Implementation. Chicago: AMA Press, 2004, p. 8.

References

Amatayakul, Margret. "Finding Quality HIPAA Security Resources." Journal of AHIMA 75, no. 1 (2004): 58–59.
Amatayakul, Margret. "Security Risk Analysis and Management: An Overview." Journal of AHIMAS 74, no. 9 (2003): 72A–72G.
Cooper, Ted et al. "CPRI Toolkit: Managing Information Security in Healthcare, Version 4." Available online at www.himss.org/asp/cpritoolkit_toolkit.asp.
CPRI Workgroup on Confidentiality, Privacy, and Security. Guidelines for Establishing Information Security Policies at Organizations Using Computer-Based Patient Record Systems. Schaumburg, IL: Computer-Based Patient Record Institute, 1995.

CPRI Workgroup on Confidentiality, Privacy, and Security. Guidelines for Managing Information Security Programs at Organizations Using Computer-Based Patient Record Systems. Schaumburg, IL: Computer-Based Patient Record Institute, 1995.

"Eight Key HIPAA Security Terms and What They Mean." HIPAA Security Compliance Insider (September 2003).
"Eight Security Compliance Tasks You Can Start Now." Health Information Compliance Insider (April 2003).
"Get Set to Comply with Final HIPAA Security Regs." Health Information Compliance Insider (April 2003).
Hjort, Beth. "Practice Brief: Security Audits (Updated)." 2003. Available in the FORE Library: HIM Body of Knowledge at www.ahima.org.
Krutz, Ronald L., and Russell Dean Vines. The CISSP Prep Guide: Gold Edition. New York: John Wiley & Sons, 2003.
National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Available online at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

Quinsey, Carol Ann. "Practice Brief: Information Security—An Overview (Updated)." 2003. Available in the FORE Library: HIM Body of Knowledge at www.ahima.org.
"Security Standards Final Rule." 45 CFR Parts 160, 162, and 164. Federal Register 68, no. 34 (February 20, 2003). Available online at www.hhs.gov/ocr/hipaa.
"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. Federal Register 65, no. 250 (August 14, 2003). Available online at www.hhs.gov/ocr/hipaa.
"Take Four Steps to Address 'Addressable' Implementation Specifications." HIPAA Security Compliance Insider (April 2003).
Prepared by
Carol Ann Quinsey, RHIA, CHPS, AHIMA professional practice

manager

Acknowledgments

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:
Quinsey, Carol Ann. "A HIPAA Security Overview" (AHIMA Practice Brief). Journal of AHIMA 75, no.4 (April 2004): 56A-C.