Summary of the HIPAA Security Rule

This is a summary of key elements of the Security Rule including who is covered, what information is protected, and what safeguards must be in place to ensure appropriate protection of electronic protected health information. Because it is an overview of the Security Rule, it does not address every detail of each provision.

Introduction

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information.[1] To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or *Standards for Privacy of Individually Identifiable Health Information*, establishes national standards for the protection of certain health information. The *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

Today, providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management, as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from wherever they are), the rise in the adoption rate of these technologies increases the potential security risks.

A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI.

This is a summary of key elements of the Security Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Privacy and Security Rules are obligated to comply with all of their applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier to review the complete requirements of the Security Rule, provisions of the Rule referenced in this summary are cited in the end notes. Visit our Security Rule section to view the entire Rule, and for additional helpful information about how the Rule applies. In the event of a conflict between this summary and the Rule, the Rule governs.

Statutory and Regulatory Background

- The *Administrative Simplification* provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Secretary of HHS to publish national standards for the security of electronic protected health information (e-PHI), electronic exchange, and the privacy and security of health information.

HIPAA called on the Secretary to issue security regulations regarding measures for protecting the integrity, confidentiality, and availability of e-PHI that is held or transmitted by covered entities. HHS developed a proposed rule and released it for public comment on August 12, 1998. The Department received approximately 2,350 public comments. The final regulation, the Security Rule, was published February 20, 2003.[2] The Rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality, integrity, and availability of e-PHI.

The text of the final regulation can be found at 45 CFR Part 160 and Part 164, Subparts A and C.

Who is Covered by the Security Rule

- The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates. For help in determining whether you are covered, use CMS's decision tool.

Read more about covered entities in the Summary of the HIPAA Privacy Rule - PDF - PDF.

Business Associates

- The HITECH Act of 2009 expanded the responsibilities of business associates under the HIPAA Security Rule. HHS developed regulations to implement and clarify these changes.

What Information is Protected

- **Electronic Protected Health Information.** The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule and here - PDF - PDF. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information "electronic protected health information" (e-PHI).[3] The Security Rule does not apply to PHI transmitted orally or in writing.

General Rules

- The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, covered entities must:

Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;

1. Identify and protect against reasonably anticipated threats to the security or integrity of the information;

2. Protect against reasonably anticipated, impermissible uses or disclosures; and

3. Ensure compliance by their workforce.[4]

The Security Rule defines "confidentiality" to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, "integrity" means that e-PHI is not altered or destroyed in an unauthorized manner. "Availability" means that e-PHI is accessible and usable on demand by an authorized person.[5]

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Therefore, when a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:

- Its size, complexity, and capabilities,

- Its technical, hardware, and software infrastructure,

- The costs of security measures, and

- The likelihood and possible impact of potential risks to e-PHI.[6]

Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.[7]

Risk Analysis and Management

- The Administrative Safeguards provisions in the Security Rule require covered entities to perform risk analysis as part of their security management processes. The risk analysis and management provisions of the Security Rule are addressed separately here because, by helping to determine which security measures are reasonable and appropriate for a particular covered entity, risk analysis affects the implementation of all of the safeguards contained in the Security Rule.

- A risk analysis process includes, but is not limited to, the following activities:

- Evaluate the likelihood and impact of potential risks to e-PHI;[8]

- Implement appropriate security measures to address the risks identified in the risk analysis;[9]
- Document the chosen security measures and, where required, the rationale for adopting those measures;[10] and
- Maintain continuous, reasonable, and appropriate security protections.[11]

Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents,[12] periodically evaluates the effectiveness of security measures put in place,[13] and regularly reevaluates potential risks to e-PHI.[14]

Administrative Safeguards

- **Security Management Process**. As explained in the previous section, a covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- **Security Personnel.** A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.[15]
- **Information Access Management.** Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).[16]
- **Workforce Training and Management.** A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI.[17] A covered entity must train all workforce members regarding its security policies and procedures,[18] and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.[19]
- **Evaluation**. A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.[20]

Physical Safeguards

- **Facility Access and Control.** A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.[21]
- **Workstation and Device Security.** A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media.[22] A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).[23]

Technical Safeguards

- **Access Control.** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).[24]

- **Audit Controls.** A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.[25]

- **Integrity Controls.** A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.[26]

- **Transmission Security.** A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.[27]

Required and Addressable Implementation Specifications

- Covered entities are required to comply with every Security Rule "Standard." However, the Security Rule categorizes certain implementation specifications within those standards as "addressable," while others are "required." The "required" implementation specifications must be implemented. The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.[28]

Organizational Requirements

- **Covered Entity Responsibilities.** If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation, the covered entity must take reasonable steps to cure the breach or end the violation.[29] Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.

- **Business Associate Contracts.** HHS developed regulations relating to business associate obligations and business associate contracts under the HITECH Act of 2009.

Policies and Procedures and Documentation Requirements

- A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.[30]

- **Updates.** A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI).[31]

State Law

- **Preemption.** In general, State laws that are contrary to the HIPAA regulations are preempted by the federal requirements, which means that the federal requirements will apply.[32] "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[33]

Enforcement and Penalties for Noncompliance

- **Compliance.** The Security Rule establishes a set of national standards for confidentiality, integrity and availability of e-PHI. The Department of Health and Human Services (HHS), Office for Civil Rights (OCR) is responsible for administering and enforcing these standards, in concert with its enforcement of the Privacy Rule, and may conduct complaint investigations and compliance reviews.

- Learn more about enforcement and penalties in the Privacy Rule Summary - PDF - PDF and on OCR's Enforcement Rule page.

Compliance Dates

- **Compliance Schedule.** All covered entities, except "small health plans," must have been compliant with the Security Rule by April 20, 2005. Small health plans had until April 20, 2006 to comply.

Copies of the Rule and Related Materials

- See our Combined Regulation Text of All Rules section of our site for the full suite of HIPAA Administrative Simplification Regulations and HIPAA for Professionals for additional guidance material.