Overview of the HIPAA Security Rule
HIPAA Security Information Paper

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule covers only protected health information (PHI) that is electronically stored or transmitted, also known as electronic protected health information (ePHI). While the HIPAA Privacy Rule is focused on protecting the confidentiality of PHI, the Security Rule broadens the focus to include protecting the integrity and availability of the information as well.

The objectives of the Security Rule are found in the general requirement that states covered entities (CEs) and business associates (BAs) that “collect, maintain, use, or transmit” ePHI must implement “reasonable and appropriate administrative, physical, and technical safeguards” that ensure integrity, availability, and confidentiality. Such measures – notably in the form of policies and procedures – must provide protection against “any reasonably anticipated threats or hazards,” ensure that the information is used and disclosed only as permitted by the Privacy Rule, and ensure that the CE’s or BA’s workforce complies with the Security Rule.

Definitions

Administrative Safeguards: Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the CE’s or BA’s workforce in relation to the protection of that information

Business Associate: A person or entity that creates, receives, maintains, or transmits PHI on behalf of a CE and is not considered a member of the CE workforce

Covered Entity: Under HIPAA, this is a health plan, a healthcare clearinghouse, or a healthcare provider that conducts one or more covered transactions in electronic form

Electronic Protected Health Information: Individually identifiable health information that is transmitted by or maintained in electronic media

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Physical Safeguards: Physical measures, policies, and procedures to protect a CE’s or BA’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion

Protected Health Information: Individually identifiable health information created or received by a CE that relates to the past, present or future physical or mental health of an individual and is transmitted or maintained in electronic, paper, or any other form. It excludes health information in employment records held by a CE in its role as an employer. PHI does not include health information of persons deceased more than 50 years

Technical Safeguards: Technology and the policy and procedures for its use that protect ePHI and control access to it

Discussion

In comparison to the HIPAA Privacy Rule, the Security Rule is logically structured and compact. The Security Rule requirements are divided into administrative, physical, and technical safeguards. Each safeguard category is divided into standards and implementation specifications that outline what a CE or BA must do to achieve the objectives presented in the general requirement.

The process used in the creation of the administrative, physical, and technical safeguards includes three parts:

1. assess potential risks and vulnerabilities to ePHI;
2. develop, implement, and maintain appropriate security measures given those risks; and
3. document those measures and keep them current.

The administrative simplification provisions of HIPAA established three characteristics the security rules needed to conform to. The Department of Health and Human Services (DHSS) created standards that were:

- “comprehensive and coordinated,” covering all aspects of security;
- “scalable” and so suitable for CEs and BAs of any size or type; and
- “technology neutral,” to allow for changes as security technologies evolve.

The last two of these characteristics enables a flexible approach that allows CEs and BAs to adopt and change protection measures based on their own needs and capabilities as the risk environment and technology changes. This also means that each CE and BA must assess its risks and protection strategies on a periodic basis to ensure its safeguards are always “reasonable and appropriate.” The rule does not permit a checklist or cookie-cutter approach to compliance “…entities affected by this regulation are so varied in terms of installed technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution or set of solutions that would be usable by all covered entities.” How a CE or BA satisfies individual security requirements and which technologies they use are “business decisions that each entity [has] to make …reviewing and modifying the measures as needed to continue the provision of reasonable and appropriate protections.”

This Rule establishes only a national “minimum standard” for security of ePHI. CEs and BAs may, for various reasons, need or want to exceed the minimum, since the Security Rule requires the protection of all ePHI, regardless of how it is used. The rule does not differentiate between internal and external transmissions, “data at rest” (stored or in process) or “data in motion” (in transmission). Security must apply to all electronic information systems. This broad applicability gives the Security Rule a unique organizational slant and accounts for the comprehensiveness of the Rule’s administrative, physical, and technical safeguard requirements.

The following is an outline of the Security Rule. For specific information on each topic see the references below or contact the DHA Privacy and Civil Liberties Office at HIPAASecurity@dha.mil.

Administrative Safeguards		
HIPAA Standard	**Section of HIPAA Security Rule**	**Section of DoD 8580.02-R**
Security Management Process	164.308(a)(1)(i)	C2.2
Assigned Security Responsibility	164.308(a)(2)	C2.3
Workforce Security	164.308(a)(3)(i)	C2.4
Information Access Management	164.308(a)(4)(i)	C2.5
Security Awareness and Training	164.308(a)(5)(i)	C2.6
Security Incident Procedures	164.308(a)(6)(i)	C2.7.1
Contingency Plan	164.308(a)(7)(i)	C2.8.1
Security Evaluation	164.308(a)(8)	C2.9
BA Contracts and Other Arrangements	164.308(b)(1)	C2.10

Physical Safeguards		
HIPAA Standard	**Section of HIPAA Security Rule**	**Section of DoD 8580.02-R**
Facility Access Controls	164.310(a)(1)	C3.2.1
Workstation Use	164.310(b)	C3.3.1
Workstation Security	164.310(c)	C3.4
Device and Media Controls	164.310(d)(1)	C3.5.1

Technical Safeguards		
HIPAA Standard	**Section of HIPAA Security Rule**	**Section of DoD 8580.02-R**
Access Controls	164.312(a)(1)	C4.2.1
Audit Controls	164.312(b)	C4.3
Integrity	164.312(c)(1)	C4.4.1
Person or Entity Authentication	164.312(d)	C4.5.
Transmission Security	164.312(e)(1)	C4.6.1

Resources/References

45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule, February 20, 2003

DoD 8580.02-R, DoD Health Information Security Regulation, July 12, 2007