Physical Safeguards

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule divides its protections into three categories: 1) administrative, 2) physical (discussed here), and 3) technical safeguards. Physical Safeguards address the physical measures, policies, and procedures required to protect a Covered Entity's (CEs) or Business Associate's (BAs) electronic information systems and related buildings and equipment. These safeguards provide protection against natural and environmental hazards, as well as unauthorized intrusions. CEs and BAs must implement safeguards that ensure compliance with the standards and implementation specifications included within the Physical Safeguards of the HIPAA Security Rule.

Definitions

Addressable: If an implementation specification is addressable, then the CE and BA must assess whether it is a reasonable and appropriate safeguard in the entity's environment. This involves analyzing the specification in reference to the likelihood of protecting the entity's electronic protected health information (ePHI) from reasonably anticipated threats and hazards. If it is reasonable, then the CE or BA should implement. If the CE or BA determines it is not reasonable and chooses not to implement an addressable specification based on its assessment, it must document the reason and implement an equivalent alternative measure that accomplishes the same end. See 45 C.F.R. § 164.306(d)(ii)(B)(2) for more information

Business Associate: A person or entity that creates, receives, maintains, or transmits protected health information (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

Implementation Specification: The specific requirements or instructions for implementing a standard

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 (PHI): 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

Required: If an implementation specification is required, then a CE and BA must implement the implementation specification

Standard: A rule, condition, or requirement that describes the classification of components; specification materials, performance, or operations; or delineation of procedures for products, systems, services or practices with respect to the privacy of individually identifiable health information

Discussion

Standards and implementation specifications that pertain to physical safeguards in both the HIPAA Security Rule and the DoD 8580.02-R "DoD Health Information Security Regulation" are presented in the table below. All standards are required and are highlighted in blue. Implementation specifications are not highlighted. Although some implementation specifications are either required or addressable under the HIPAA Security Rule, ***all*** implementation specifications are required under DoD 8580.02-R. (See Information Paper on SPECIFICATIONS: STANDARDS AND IMPLEMENTATIONS).

PHYSICAL SAFEGUARDS

R = Required, A = Addressable

■ =Standards, □ =Implementation Specifications

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	Required?	
				HIPAA	DOD
164.310(a)(1)	Facility Access Controls	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	C3.2.1	R	R
164.310(a)(2)(i)	Contingency Operations	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	C3.2.3	A	R
164.310(a)(2)(ii)	Facility Security Plan	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	C3.2.4	A	R

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	Required?	
				HIPAA	DOD
164.310(a)(2)(iii)	Access Control and Validation Procedures	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	C3.2.5	A	R
164.310(a)(2)(iv)	Maintenance Records	Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).	C3.2.6	A	R
164.310(b)	Workstation Use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.	C3.3.1	R	R
164.310(c)	Workstation Security	Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	C3.4	R	R
164.310(d)(1)	Device and Media Controls	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	C3.5.1	R	R
164.310(d)(2)(i)	Disposal	Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	C3.5.3	R	R
164.310(d)(2)(ii)	Media Re-Use	Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.	C3.5.4	R	R
164.310(d)(2)(iii)	Accountability	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	C3.5.5	A	R
164.310(d)(2)(iv)	Data Backup and Storage	Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	C3.5.6	A	R

Resources/References

45 CFR 164.310, Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule

DoD 8580.02-R, DoD Health Information Security Regulation, July 12, 2007, C3