Technical Safeguards

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule divides its protections into three categories: 1) administrative, 2) physical, and 3) technical (discussed here) safeguards. Technical safeguards are the technologies and related policies and procedures that protect electronic protected health information (ePHI) that is created, processed, stored, or transmitted by a Covered Entity (CE) or Business Associate (BA). CEs and BAs must implement safeguards that ensure compliance with the standards and implementation specifications included within the Technical 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 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

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

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

Discussion

Standards and implementation specifications that pertain to technical 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. The implementation specifications are not highlighted, and are either required or addressable. (See Information Paper on SPECIFICATIONS: STANDARDS AND IMPLEMENTATIONS).

TECHNICAL 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
164.312(a)(1)	Access Controls	Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.	C4.2.1	R	R
164.312(a)(2)(i)	Unique User Identification	Assign a unique name and/or number for identifying and tracking user identity.	C4.2.2	R	R
164.312(a)(2)(ii)	Emergency Access Procedure	Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	C4.2.3	R	R
164.312(a)(2)(iii)	Automatic Logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	C4.2.4	A	A
164.312(a)(2)(iv)	Encryption and Decryption	Implement a mechanism to encrypt and decrypt ePHI.	C4.2.5	A	A
164.312(b)	Audit Controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	C4.3	R	R

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	Required?	
				HIPAA	DOD
164.312(c)(1)	Integrity	Implement policies and procedures to protect ePHI from improper alteration or destruction.	C4.4.1	R	R
164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information	Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	C4.4.2	A	R
164.312(d)	Person or Entity Authentication	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	C4.5	R	R
164.312(e)(1)	Transmission Security	Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	C4.6.1	R	R
164.312(e)(2)(i)	Integrity Controls	Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	C4.6.2	A	R
164.312(e)(2)(ii)	Encryption	Implement a mechanism to encrypt ePHI whenever deemed appropriate.	C4.6.3	A	A

Resources/References

45 CFR 164.312, Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule

DoD 8580.02-R, DoD Health Information Security Regulation, July 12, 2007, C4