Administrative Safeguards

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule divides its protections into three categories: 1) administrative (discussed here), 2) physical, and 3) technical safeguards. Administrative Safeguards are designed to protect electronic protected health information (ePHI) and to manage the conduct of the covered entity's (CE) workforce and its business associates (BAs) using ePHI in the performance of their jobs. CEs and BAs must implement safeguards that ensure compliance with the standards and implementation specifications included within the Administrative 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

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 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

Discussion

Standards and implementation specifications that pertain to administrative 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).

ADMINISTRATIVE 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
164.308(a)(1)(i)	Security Management Process	Implement policies and procedures to prevent, detect, contain, and correct security violations.	C2.2	R	R
164.308(a)(1)(ii)(A)	Risk Analysis	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the CE or BA.	C2.2.3	R	R
164.308(a)(1)(ii)(B)	Risk Management	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).	C2.2.4	R	R

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	Required?	
				HIPAA	DOD
164.308(a)(1)(ii)(C)	Sanction Policy	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the CE or BA.	C2.2.5	R	R
164.308(a)(1)(ii)(D)	Information System Activity Review	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	C2.2.6	R	R
164.308(a)(2)	Assigned Security Responsibility	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the CE or BA.	C2.3	R	R
164.308(a)(3)(i)	Workforce Security	Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to ePHI.	C2.4	R	R
164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	C2.4.3	A	R
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Implement procedures to determine that the access of a workforce member to ePHI is appropriate.	C2.4.4	A	R
164.308(a)(3)(ii)(C)	Termination Procedure	Implement procedures for terminating access to ePHI when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	C2.4.5	A	R
164.308(a)(4)(i)	Information Access Management	Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of subpart E of this part.	C2.5	R	R

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	Required?	
				HIPAA	DOD
164.308(a)(4)(ii)(A)	Isolating Healthcare Clearinghouse Function	If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.	N/A	R	N/A
164.308(a)(4)(ii)(B)	Access Authorization	Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	C2.5.4	A	R
164.308(a)(4)(ii)(C)	Access Establishment and Modification	Implement policies and procedures that, based upon the CE's or BA's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	C2.5.5	A	R
164.308(a)(5)(i)	Security Awareness and Training	Implement a security awareness and training program for all members of its workforce (including management).	C2.6	R	R
164.308(a)(5)(ii)(A)	Security Reminders	Implement periodic security updates.	C2.6.4	A	R
164.308(a)(5)(ii)(B)	Protection from Malicious Software	Implement procedures for guarding against, detecting, and reporting malicious software.	C2.6.5	A	R
164.308(a)(5)(ii)(C)	Log-in Monitoring	Implement procedures for monitoring log-in attempts and reporting discrepancies.	C2.6.6	A	R
164.308(a)(5)(ii)(D)	Password Management	Implement procedures for creating, changing, and safeguarding passwords.	C2.6.7	A	R
164.308(a)(6)(i)	Security Incident Procedures	Implement policies and procedures to address security incidents.	C2.7.1	R	R
164.308(a)(6)(ii)	Response and Reporting	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the CE or BA; and document security incidents and their outcomes.	C2.7.2	R	R

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	Required?	
				HIPAA	DOD
164.308(a)(7)(i)	Contingency Plan	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	C2.8.1	R	R
164.308(a)(7)(ii)(A)	Data Backup Plan	Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	C2.8.2	R	R
164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Establish (and implement as needed) procedures to restore any loss of data.	C2.8.3	R	R
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	C2.8.4	R	R
164.308(a)(7)(ii)(D)	Testing and Revision Procedure	Implement procedures for periodic testing and revision of contingency plans.	C2.8.5	A	R
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Assess the relative criticality of specific applications and data in support of other contingency plan components.	C2.8.6	A	R
164.308(a)(8)	Evaluation	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI that establishes the extent to which a CE's or BA's security policies and procedures meet the requirements of this subpart.	C2.9 (C2.9.1 - C2.9.3)	R	R
164.308(b)(1)	Business Associate Contracts and Other Arrangements	A CE may permit a BA to create, receive, maintain, or transmit ePHI on the CE's behalf only if the CE obtains satisfactory assurances, in accordance with Sec. 164.314(a), that the BA will appropriately safeguard the information. A CE is not required to obtain such satisfactory assurances from a BA that is a subcontractor.	C2.10	R	R

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	Required?	
				HIPAA	DOD
164.308(b)(3)	Written Contract or Other Arrangement	Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the BA that meets the applicable requirements of Sec. 164.314(a).	C2.10.1	R	R
164.316 (a)	Policies and procedures	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in Sec. 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A CE or BA may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	C1.6	R	R
164.316(b)(1)	Documentation	A CE must, in accordance with §164.306: (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity or assessment.	C1.6.4.4, C1.6.4.5	R	R
164.316(b)(2)(i)	Time Limit	Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	C1.6.4.5.1	R	R
164.316(b)(2)(ii)	Availability	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	C1.6.4.5.2	R	R
164.316(b)(2)(iii)	Updates	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	C1.6.4.5.3	R	R

Resources/References

45 CFR 164.308, Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule

DoD 8580.02-R, DoD Health Information Security Regulation, July 12, 2007, C2