Specifications: Standards & Implementation

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities (CEs) and business associates (BAs) to have in place appropriate administrative, physical, and technical safeguards. These safeguards are employed to protect electronic protected health information (ePHI). Under the Security Rule, each set of safeguards is comprised of a number of standards that CEs and BAs are required to meet, along with a number of implementation specifications that are either required or addressable.

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: 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

Reasonableness: The appropriate measures CEs and BAs must institute to avert anticipated risks to their ePHI which take into consideration the following factors:

1. The size, complexity, and capabilities of the organization;

2. The organization's technical infrastructure, hardware, and software security capabilities;
3. The costs of the security measures; and
4. The probability and criticality of potential risks to ePHI

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

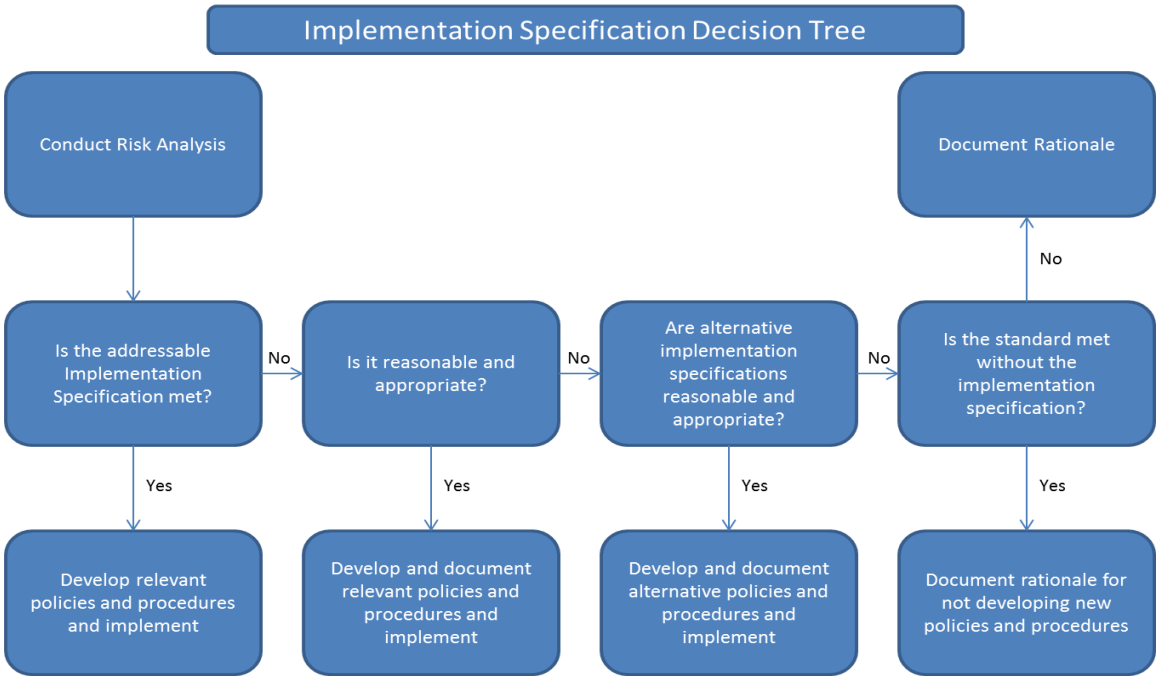
The HIPAA Security Rule requires CEs and BAs to have appropriate administrative, physical, and technical safeguards in place to protect ePHI. Each of these safeguards is comprised of standards and implementation specifications. Under DoD 8580.02-R all standards are required and all but three (3) of the Technical Safeguard implementation specifications are required.

If an implementation specification is required, the CE or BA must implement policies and/or procedures that meet what the implementation specification requires. If an implementation specification is addressable, then the CE or 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 CE's or BA's ePHI from reasonably anticipated threats and hazards. If the CE or BA chooses not to implement an addressable specification based on its assessment, the CE or BA must then document the reason and, if reasonable and appropriate, implement an equivalent alternative measure. See CFR § 164.306(d)(ii)(B)(2) for more information.

Under DoD 8580.02-R, there are three (3) implementation specifications that are addressable: Automatic Logoff, Encryption and Decryption (with regard to access of wireless and mobile devices, and data at rest) under the Access Control Standard, and Encryption (with regard to data in transit) under the Transmission Security Standard. Additional DoD policy will affect a CE's or BA's analysis of these addressable implementation specifications. It is recommended that CEs and BAs consult with the office or individual responsible for implementing DoD Information Assurance (IA) policies (e.g., Chief Information Officer (CIO)) to ensure that minimum organizational requirements are met.

Notwithstanding other DoD policies, CEs and BAs must comply with the Security Rule and the process described above, to either implement these three controls, document and implement alternative controls, or if the standard can be met without implementing controls, document the rationale.

The following chart can assist CEs and BAs in making this determination:



Factors to consider when determining if the implementation specification or alternate safeguard is reasonable and appropriate include the degree of risk as determined through the risk assessment, cost of implementing the safeguard, capabilities of the hardware, software and technical infrastructure, your business processes, other safeguards already in place, and the size, complexity, and capabilities of the CE or BA.

A full list of all of the Administrative, Physical, and Technical safeguards, as well as their standards and implementation specifications can be found in the Administrative Safeguards Information Paper, the Physical Safeguards Information Paper, and the Technical Safeguards Information Paper.

Resources/References

45 CFR 164.306(d), Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule

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