HIPAA security rule & risk analysis

The HIPAA Security Rule requires physicians to protect patients' electronically stored, protected health information (known as “ePHI”) by using appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of this information. Essentially, the Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and nontechnical safeguards that covered entities must implement to secure ePHI.

All covered entities must assess their security risks, even those entities who utilize certified electronic health record (EHR) technology. Those entities must put in place administrative, physical and technical safeguards to maintain compliance with the Security Rule and document every security compliance measure.

Administrative safeguards

HIPAA defines administrative safeguards as, “Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.” (45 C.F.R. § 164.304).

These are, like the definition says, policies and procedures that set out what the covered entity does to protect its PHI. Rather than actual physical safeguards or technical requirements, these requirements cover training and procedures for employees of the entity, whether or not they have direct access to PHI.

Physical safeguards

Physical safeguards involve access both to the physical structures of a covered entity and its electronic equipment (45 CFR §164.310). ePHI and the computer systems in which it resides must be protected from unauthorized access, in accordance with defined policies and procedures. Some of these requirements can be accomplished by using electronic security systems, but physicians should not rely on use of certified electronic health records technology (CEHRT) to satisfy their Security Rule compliance obligations.

URL: https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis
Copyright 1995 - 2021 American Medical Association. All rights reserved.

Technical safeguards

Technical safeguards encompass the technology, as well and the policies and procedures for its use, that protect ePHI and control access to it. They are often the most difficult regulations to comprehend and implement (45 CFR §164.312).

A flexible approach

The Security Rule incorporates the concepts of scalability, flexibility and generalization. In other words, the regulations do not expect the same security precautions from small or rural providers as are demanded of large covered entities with significant resources. Security is recognized as an evolving target, and so HIPAA's security requirements are not linked to specific technologies or products. HHS has stated it is focused more on what needs to be done and less on how it should be accomplished.

The security regulations consist of a 3-tiered system of requirements. First, there is a series of standards, legal requirements that all entities are expected to meet. Second, there may be implementation specifications that provide detailed instructions and steps to take in order to be in compliance with the standard.

In an effort to make the Security Rule more flexible and applicable to covered entities of all sizes, some implementation specifications are required, while others are only addressable. Required implementation specifications must be implemented by all covered entities. Addressable implementation specifications require a covered entity to assess whether the specification is a reasonable and appropriate safeguard in the entity's environment.

If the specification is reasonable and appropriate, the covered entity must implement the specification. If a covered entity determines that an addressable implementation specification is not reasonable and appropriate, it must document its assessment and basis for its decision and implement an alternative mechanism to meet the standard addressed by the implementation specification.

Risk assessment

URL: https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis
Copyright 1995 - 2021 American Medical Association. All rights reserved.

To comply with the Security Rule's implementation specifications, covered entities are required to conduct a risk assessment to determine the threats or hazards to the security of ePHI and implement measures to protect against these threats and such uses and disclosures of information that are not permitted by the Privacy Rule.

A risk assessment should be tailored to the covered entity's circumstances and environment, including the following:

- Size, complexity and capabilities of the covered entity
- The covered entity's technical infrastructure, hardware and software security capabilities
- The probability and criticality of potential risks to ePHI
- The costs of security measures

Note, however, that HHS has made it clear that cost alone is not a sufficient basis for refusing to adopt a standard or an addressable implementation specification. Fortunately, the rules are not prescriptive and a number of tactics can achieve compliance. To assist physicians with the risk-assessment process, the U.S. Department of Health & Human Services (HHS) Office of Civil Rights has developed a downloadable "Security risk assessment tool."

- AMA's SL2 series: Security risk analysis
  This webinar was first presented on Sept. 13, 2017. Listen to it again by registering at the link.

Required documentation

Behind every security compliance measure is a documentation requirement. Practically every facet of HIPAA compliance requires that policies and procedures be created and implemented. These documents must be retained for at least six years (and state requirements may mandate longer retention periods).

Policies may be changed at any time, so long as the accompanying documentation is also updated. Regulations require periodic review of policies and responses to changes in the ePHI environment.

- AMA Education Center: HIPAA security rule compliance through effective risk assessment
- Guide to Privacy and Security of Health Information (PDF)
- Health information technology
- HIPAA privacy and security toolkit: Helping your practice meet compliance requirements (PDF)
- HIPAA security rule: FAQs regarding encryption of personal health information (PDF)

This resource is provided for informational and reference purposes only and should not be construed as the legal advice of the American Medical Association. Specific legal questions regarding this

URL: https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis
Copyright 1995 - 2021 American Medical Association. All rights reserved.

information should be addressed by one's own counsel.

URL: https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis
Copyright 1995 - 2021 American Medical Association. All rights reserved.