Haekka

Lesson 6 | HIPAA Security Rule

Updated 2020-09-12

HIPAA - Security Rule

The Security Rule defines the technical requirements of HIPAA. Like many compliance regimes, it is heavily aligned with NIST security standards. The Security Rule is divided into three categories of requirements - 1) Administrative, 2) Physical, and 3) Technical.

Requirements in the HIPAA Security Rule are either Required or Addressable, which is a bit confusing because all of the HIPAA requirements are actually required. The main difference between Required and Addressable is that Addressable requirements can be met with other, mitigating controls.

Administrative Safeguards

Risk Assessment

Under HIPAA, every organization must assess the risk to PHI. The process involves identifying threats, risk, and impacts to an organization if PHI is breached. Mitigating controls should be established and documented for all risks.

This should be done on a regular basis. As a rule of thumb, a risk assessment should be performed on a regular, annual cadence as well as with significant changes to procedures or technologies.

The definitive guide on performing risk assessments and managing risk is NIST - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Security Personnel

Similar to the Privacy Rule personnel requirement, an individual needs to be appointed to create and maintain security policies and procedures.

Information Access

Role-based access policies and procedures need to be implemented. HIPAA audits frown on shared accounts, even privileged accounts like root or admin. All accounts should be assigned to individuals and only individuals that need access to PHI should be granted access to PHI.

Workforce Training

All workforce members have to be trained in security policies and procedures. In practical, day-to-day work, specific procedures and types of security implementations (backups schedules, encryption standards, etc) should be readily accessible to ensure ongoing compliance.

Evaluation

Organizations need to do regular assessments of how their security posture aligns with the Security Rule. Some form of regular, external audit, vulnerability assessment, and/or penetration test should be performed as a part of ongoing evaluation.

Physical Safeguards

Facility Access

Access to physical facilities (offices, data centers, etc) needs to be restricted. In the case of cloud-based technology, this is addressed by the cloud services provider (AWS, Microsoft Azure, etc).

Device Security

Computers and other devices that access PHI or systems with access to PHI need to be secured. This falls under the bucket of endpoint or perimeter security.

Technical Safeguards

Access Management

Technical security controls need to be implemented to secure technology that has access to PHI.

Audit Controls

Tools need to be implemented to log access to systems and data.

Integrity Controls

PHI needs to be monitored to ensure it is not improperly modified or deleted

Data Transmission

Data in transit needs to be secured. The most common means is through end-to-end encryption.

The Security Rule defines the ways in which an organization is required to implement the technical controls and procedures.