Data Security Policy – HIPAA Security Rule Basics

PURPOSE

To provide an overview of the HIPAA Security Rule and its requirements.

SCOPE

The HIPAA Security Rule Basics Policy covers Organization's

- Basic obligations under the HIPAA Security Rule
- Designated Security Official
- Required versus Addressable standard components
- Roles and Responsibilities
- Relevant Regulations, Standards, and Criteria

POLICY

The HIPAA Security Rule requires in-scope organizations such as Covered Entities and certain Business Associates to protect the CIA triad of confidentiality, integrity, and availability of electronic protected health information (ePHI). These combined technical, administrative, and physical measures are designed to safeguard PHI and ePHI.

Organization has set up policies and procedures to carry out the requirements of the HIPAA Security Rule, including responding to and reporting security incidents. These policies and procedures are retained in written form and reviewed and updated periodically.

Basic Requirements of the Security Rule

Under the HIPAA Security Rule, the Organization must:

- Ensure the confidentiality, integrity, and availability of ePHI that the company creates, processes, receives, or transmits
- Prevent and address any threats to the security or integrity of ePHI
- Prevent against unauthorized disclosure of ePHI
- Enforce compliance with the HIPAA Security Rule across the company's workforce

Designated Security Official

Organization has appointed a designated Security Official to develop and enforce the company's data security policies and procedures. The Security Official should be sufficiently senior in the company. The designated Security Official is listed below:

Name:

Title:

Email or Phone:

Required vs Addressable Standards

The HIPAA Security Rule standards include required and addressable components.

Organization sets up appropriate controls for required components, taking into account the company's current resources and capabilities, as well as potential risks to *ePHI.*

Organization assesses addressable components for feasibility. If the component can be addressed by Organization, the company will set up appropriate controls. If the component cannot be feasibly addressed, the reasons will be documented and retained.

Definitions

Administrative Safeguards - The HIPAA Security Rule *administrative safeguards* consist of administrative actions, policies, and procedures. These actions, policies, and procedures are used to manage the selection, development, and implementation of security measures.

The *administrative safeguards* regulation can be found at 45 C.F.R 164.308. This provision is subdivided into 45 CFR 164.308(a) and 45 CFR 164.308(b).

Physical Safeguard - Physical safeguards protect the physical security of offices and other locations where *ePHI* may be stored or maintained. Common examples of *physical safeguards* include:

- Alarm systems
- Surveillance cameras
- Access control systems
- Security systems
- Locking of areas where *ePHI* is stored

Technical Safeguards- Technical safeguards include measures, such as endpoint protection, firewalls, encryption, and data backup, that ensure that ePHI is properly accessed, monitored, and maintained.

ROLES AND RESPONSIBILITIES

Security Official: Sets up and enforces security policies and procedures in accordance with the HIPAA Security Rule. Reviews relevant policies and updates documentation as needed. Oversees incident response and reporting mechanisms. Main point of contact for security-related communications.

VIOLATIONS

Failure to comply with the HIPAA Security Rule or Organization's policies and procedures may result in disciplinary action or sanctions.

RELEVANT HIPAA REGULATIONS

- 45 CFR §164.308 *Administrative safeguards*
- 45 CFR §164.308(a)(2) *Assigned security responsibility*
- 45 CFR §164.310 *Physical safeguards*
- 45 CFR §164.312 *Technical safeguards*