Purpose

[YOUR COMPANY’S NAME HERE] is committed to ensuring the privacy and security of protected health information. In order to manage the facilitation and implementation of activities related to the privacy and security of protected health information, [YOUR COMPANY’S NAME HERE] will appoint and maintain an internal HIPAA Security Officer position.

As required in 45 C.F.R. § 164.308(a)(2), Assigned Security Responsibility, the purpose of this policy is to establish how the HIPAA Security Officer will serve as the focal point for security compliance-related activities and responsibilities, as listed below. The final responsibility for the implementation and maintenance of the security program must rest with one individual. In general, the HIPAA Security Officer is charged with developing, maintaining, and implementing organizational policies and procedures, conducting educational programs, reviewing conduct of those assigned security responsibilities, and administering reviews relating to the company’s security program.

Definitions

Reference [YOUR COMPANY’S NAME HERE]’s “HIPAA-HITECH Privacy and Security Glossary”.
HIPAA Security Rule Policies

Policy
[YOUR COMPANY NAME HERE] will identify the security official who is responsible for the development and implementation of the policies and procedures required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and, specifically, Subpart C Security Standards for the protection of electronic protected health information (ePHI) of PART 164 – Security and Privacy.

Procedures:

Qualifications
1. The HIPAA Security Officer must demonstrate familiarity with the legal requirements relating to privacy and health care operations, as well as the ability to communicate effectively with and coordinate the efforts of technology and non-technology personnel. Information security will cover legal issues, hardware and software security, as well as physical security.
2. [OPTIONAL: It is desirable that the HIPAA Security Officer has a background to include the following:
   (a) Bachelor’s degree or higher from an accredited university in Management Information Systems, Computer Science, Business Administration or similar discipline;
   (b) Security certification (e.g., Certified Information Systems Security Professional (CISSP));
   (c) Minimum of three years of information security experience].

Identification and Replacement
1. The current HIPAA Security Officer is:
   • Name and Title
   • Office Phone Number
   • Fax Phone Number
   • Home Phone Number
   • Business Address
HIPAA Security Rule Policies

- Business E-Mail Address

2. The backup SECURITY OFFICER is:
   - Name and Title
   - Office Phone Number
   - Fax Phone Number
   - Home Phone Number
   - Business Address
   - Business E-Mail Address

3. In the event that the HIPAA Security Officer needs to be replaced, the backup HIPAA Security Officer will be the interim HIPAA Security Officer. A search for a replacement HIPAA Security Officer will be conducted and the position filled as soon as possible. Final determination of a new HIPAA Security Officer will be made by [YOUR COMPANY’S NAME HERE] Chief Executive Officer.

4. All workforce members will be made aware of the HIPAA Security Officer’s identity, as well as the HIPAA Security Officer’s role and responsibilities. Any HIPAA Security Officer changes will be promptly communicated.

Responsibilities

1. The HIPAA Security Officer leads in the development, awareness and enforcement of information security policies and procedures, measures and mechanisms to ensure prevention, detection, containment, and correction of security incidents. He/she will also ensure that the policy/procedure requirements comply with statutory and regulatory requirements regarding security of EPHI.

2. The HIPAA Security Officer maintains security policies that include:
   (a) Administrative Safeguards: Formal mechanisms for risk analysis and management, information access controls, and appropriate sanctions for failure to comply.
HIPAA Security Rule Policies

(b) **Physical Safeguards:** Ensure assigned security responsibilities, control access to media (e.g., diskettes, tapes, backups, disposal of data), protect against hazards and unauthorized access to computer systems, and secure workstation locations and use. The HIPAA Security Officer may co-ordinate with the building security or facilities management personnel for this purpose.

(c) **Technical Safeguards:** Establish access controls, emergency procedures, authorization controls, and data/entity access and authentication.

3. The HIPAA Security Officer maintains security procedures that include:
   (a) Evaluation of compliance with security measures.
   (b) Contingency plans for emergencies and disaster recovery.
   (c) Security incident response process and protocols.
   (d) Testing of security procedures, measures and mechanisms, and continuous improvement.
   (e) Security incident reporting mechanisms and sanction policy.
   (f) Proper documentation of security incidents and the responses to them.

4. The HIPAA Security Officer maintains appropriate security measures and mechanisms to guard against unauthorized access to electronically stored and/or transmitted patient data and protect against reasonably anticipated threats and hazards, for example:
   (a) Integrity controls.
   (b) Authentication controls.
   (c) Access controls.
   (d) Encryption.
   (e) Abnormal condition alarms, audit trails, entity authentication, and event reporting.
HIPAA Security Rule Policies

5. The HIPAA Security Officer oversees and/or performs on-going security monitoring of organization information systems
6. The HIPAA Security Officer is responsible for directing or conducting periodic risk assessments as your systems or processes change or new ones are added. He/she will also be responsible for obtaining sign-off from appropriate management for acceptance of residual risks.
7. The HIPAA Security Officer will conduct functionality and gap analyses to determine the extent to which key business areas and infrastructure comply with statutory and regulatory requirements.
8. The HIPAA Security Officer will evaluate and recommend new information security technologies and counter-measures against threats to information or privacy.
9. The HIPAA Security Officer ensures ongoing compliance through suitable training/awareness programs and periodic security audits.
10. The HIPAA Security Officer serves as a resource regarding matters of informational security, and on a periodic basis, reports the status of information security activities to the [Executive Compliance Committee].
11. The HIPAA Security Officer will ensure that security concerns have been addressed in system implementations including EHRs and any exchange of health information with patients and outside entities.

Regulatory Authority

45 C.F.R. §164.308(a) (2) Administrative Safeguards

(a) A covered entity* must, in accordance with § 164.306:

  2. Standard: Assigned security responsibility. Identify the HIPAA Security Officer who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
HIPAA Security Rule Policies

* Note: Pursuant to the HITECH Act, HIPAA Business Associates also need with to comply with the requirements of the HIPAA Security Rule.

**Analysis, Background, and Implications**

The objective of this standard is to identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. Assigned security responsibility is the practice established by management to administer and supervise the execution and use of security measures to protect data, and to manage and supervise the conduct of the workforce in relation to the protection of data.

The final Security Rule requires that the final responsibility for a covered entity’s security must be assigned to one official – this is to **ensure accountability**. More than one individual may be given specific security responsibilities, especially within a large organization, but a single individual must be designated as having the overall responsibility for the security of the entity’s electronic PHI. Depending on the size of the organization and other factors, it is possible for the same person to fill the role for both security and privacy.

Implementation is expected to vary widely depending on the size and nature of the covered entity, with small offices assigning this as an additional duty to an existing staff person, large organizations creating a full-time HIPAA Security Officer or designating both the Security and Privacy official responsibilities to one individual. Regardless of the division of responsibilities, however, the ultimate responsibility for the security program, which is to bring the organization into compliance with the Final HIPAA Security rule, must rest with one individual. The HIPAA Security Officer is charged with overseeing the placement of the appropriate technical, organizational and administrative safeguards as well as enforcing the program and reviewing the conduct of those responsible for protecting EPHI for the organization.
HIPAA Security Rule Policies

References

Internal

2. Policy #2. Risk Analysis
3. Policy #3. Risk Management
4. Policy #4. Sanction Policy

External