Purpose

This policy is designed to establish [YOUR COMPANY NAME HERE]’s commitment to conducting business in compliance with all applicable laws, regulations and [YOUR COMPANY NAME HERE] policies related to 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. [YOUR COMPANY NAME HERE] has adopted this policy to ensure that security violations are prevented, detected, contained and corrected in accordance with section § 164.308(a)(1) of the HIPAA Security Rule.

This policy provides high level requirement, responsibilities and procedures related to the Security Management Process at [YOUR COMPANY NAME HERE]. This policy is further supported by the following four policies for the four implementation specifications under the “Security Management Process” Standard.

1. Policy #2. Risk Analysis
2. Policy #3. Risk Management
3. Policy #4. Sanction Policy
4. Policy #5. Information Systems Activity Review
HIPAA Security Rule Policies

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

Policy
1. [YOUR COMPANY NAME HERE] will identify all information systems that house ePHI including all assets (e.g., hardware, software, applications, information/data sets) that are used to collect, store, process, or transmit ePHI. The information systems must be identified regardless of whether they are hosted on premise or off premise with a service provider or perhaps an application that is hosted in the cloud.

2. [YOUR COMPANY NAME HERE] will analyze business functions and verify ownership and control of information system elements as necessary.

3. [YOUR COMPANY NAME HERE] will implement policies and procedures to prevent, detect, contain, and correct security violations, which are designed to comply with the standards, implementation specifications, or other requirements of the HIPAA Security regulations.

4. [YOUR COMPANY NAME HERE] will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity (CE) or Business Associate (BA) (as applicable).

5. [YOUR COMPANY NAME HERE] will implement security risk management measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306 Security standards: General rules. (a) General requirements.
HIPAA Security Rule Policies

6. [YOUR COMPANY NAME HERE] will implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports to maintain ongoing understanding of activity in information systems that create, maintain, process or transmit ePHI.

7. [YOUR COMPANY NAME HERE] will incorporate into its Security Management Process policies, procedures and other administrative documents any changes in law.

8. [YOUR COMPANY NAME HERE] will properly document and implement any Security Management Process actions, activities and assessments as necessary by law.

9. [YOUR COMPANY NAME HERE] will implement appropriate required implementation specifications based on size, complexity, and capabilities, as well as technical infrastructure, hardware, and software security capabilities, cost, and risk analysis.

10. [YOUR COMPANY NAME HERE] will decide what addressable implementation specifications are reasonable and appropriate based on size, complexity, and capabilities, as well as technical infrastructure, hardware, and software security capabilities, cost, and risk analysis.

11. [YOUR COMPANY NAME HERE] will implement addressable implementation specifications determined to be reasonable and appropriate. If implementing an addressable implementation specification is not reasonable and appropriate, [YOUR COMPANY NAME HERE] will: (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and (2) Implement an equivalent alternative measure if reasonable and appropriate.
HIPAA Security Rule Policies

Procedures

1. [YOUR COMPANY NAME HERE]’s HIPAA Security Officer (Refer Policy # 6. Assigned Security Responsibility) will direct and manage the organization’s Security Management program and operations.

2. [YOUR COMPANY NAME HERE]’s HIPAA Security Officer will maintain an inventory of ePHI systems and devices including all hardware and software that are used to collect, store, process, or transmit ePHI. The information systems must be identified regardless of whether they are hosted on premise or off premise with a service provider or perhaps an application that is hosted in the cloud.

3. [YOUR COMPANY NAME HERE]’s HIPAA Security Officer will direct or perform a criticality analysis (see Contingency Plan policies and procedures) and determine the value and relative desired assurance levels for each asset identified above. Consider the levels desired for confidentiality, integrity and availability. Ensure that ePHI components are identified and included.

4. [YOUR COMPANY NAME HERE]’s HIPAA Security Officer will analyze business functions from time to time and verify ownership and control of information system elements as necessary.

5. [YOUR COMPANY NAME HERE]’s HIPAA Security Officer (Refer Policy # 6. Assigned Security Responsibility) will direct or conduct an accurate and thorough assessment of the risks to the confidentiality, integrity, and availability of ePHI. A separate Risk Analysis Policy and Procedure (Refer Policy # 2. Risk Analysis) details the procedural steps that are followed to implement this specification.

6. [YOUR COMPANY NAME HERE] will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). A separate Risk Management Policy and Procedure (HIPAA Security Policy #3) details the procedural steps that are followed to implement this specification.
HIPAA Security Rule Policies

7. [YOUR COMPANY NAME HERE] will apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. A separate Sanction Policy and Procedure (HIPAA Security Policy #4) details the procedural steps that are followed to implement this specification.

8. [YOUR COMPANY NAME HERE] will implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. A separate Information System Activity Review Policy and Procedure (HIPAA Security Policy #5) details the procedural steps that are followed to implement this specification.

9. [YOUR COMPANY NAME HERE] will maintain in written form (paper and/or electronic) the documentation of appropriate aspects of the Security Management Process for regulatory compliance.

10. [YOUR COMPANY NAME HERE] will continually monitor for events (in accordance with the above policy) that would necessitate policy and procedure or documentation revision.

11. [YOUR COMPANY NAME HERE] will make changes to existing documents to address these events. Include revision information, to include change summaries, in each new document version.

12. [YOUR COMPANY NAME HERE] will hold a review of this policy and procedures to include [ROLE 1], [ROLE 2], and [ROLE N], e.g. HIPAA Security Officer, Information and Technology Service Coordinator, (ITS Coordinator), Human Resource Coordinator (HR Coordinator). Ensure that [YOUR COMPANY NAME HERE]’s Security Management Process policy have been reasonably designed to take into account the size and type of activities undertaken by [YOUR COMPANY NAME HERE] with respect to ePHI.
HIPAA Security Rule Policies

13. [YOUR COMPANY NAME HERE] will disseminate all official updates to this policy and procedure to the workforce as applicable within [PERIOD] of any changes.

14. This policy and procedure will be maintained in a manner that allows necessary availability, while also ensuring the security of information.

*Regulatory Authority*

45 C.F.R. §164.308(a)(1)(i) **Standard: Security Management Process**

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

1(1)(i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
HIPAA Security Rule Policies

**Analysis, Background, and Implications**

The security management process standard requires covered entities to implement policies and procedures to prevent, detect, contain, and correct security violations.

The heart of any viable information security program is a clearly articulated security management process which includes risk analysis as a starting, foundational step. All HIPAA Security policies and procedures play a vital role in assuring the confidentiality, integrity and availability of ePHI. However, the Security Management Process policy and related procedures represent an organization’s overall security strategy.

As cited in Guidance on Risk Analysis from Health and Human Services, conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before the Office for Civil Rights (OCR) can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

All ePHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of ePHI. Risk analysis is the first step in that process.

The Security Rule does not prescribe a specific risk analysis methodology, recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization. Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve.
HIPAA Security Rule Policies

References

Internal

1. Policy #2. Risk Analysis
2. Policy #3. Risk Management
3. Policy #4. Sanction Policy
4. Policy #5. Information Systems Activity Review
5. Policy #6. Assigned Security Responsibility

External