HIPAA - Security Rule

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

30	HIPAA 164.310(b) - Workstation Use
31	HIPAA 164.310(c) - Workstation Security
32	HIPAA 164.310(d)(2)(i) - Media Disposal
33	HIPAA 164.310(d)(2)(ii) - Media Re-use
34	HIPAA 164.310(d)(2)(iii) - Media Accountability
35	HIPAA 164.310(d)(2)(iv) - Data Backup and Storage (during transfer)
36	HIPAA 164.312(a)(2)(i) - Unique User Identification
37	HIPAA 164.312(a)(2)(ii) - Emergency Access Procedure
38	HIPAA 164.312(a)(2)(iii) - Automatic Logoff
39	HIPAA 164.312(a)(2)(iv) - Encryption and Decryption (data at rest)
40	HIPAA 164.312(b) - Audit Controls
41	HIPAA 164.312(c)(1) - Protection Policies/Procedures Against Improper Data Alteration or Destruction
42	HIPAA 164.312(c)(2) - Protection Mechanism Against Improper Data Alteration or Destruction
43	HIPAA 164.312(d) - Person or Entity Authentication
44	HIPAA 164.312(e)(2)(i) - Protection of Data During Transmission
45	HIPAA 164.312(e)(2)(ii) - Integrity Controls & Encryption
46	HIPAA 164.314(a)(1) - Business Associate Contracts
47	HIPAA 164.316(a) - Policies and Procedures
48	HIPAA 164.316(b)(1) - Documentation
49	HIPAA 164.316(b)(2)(i) - Time Limit
50	HIPAA 164.316(b)(2)(ii) - Availability
51	HIPAA 164.316(b)(2)(iii) - Updates

Purpose

The purpose is to ensure that healthcare providers and health plans that qualify as HIPAA Covered Entities, and qualifying vendors and partners that qualify as HIPAA Business Associates, meet all the requirements defined in HIPAA and associated guidance.

Scope

This policy applies to the workforce members of organizations and business associates who come in contact with verbal, written, or electronic Protected Health Information (PHI).

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

HIPAA 164.308(a)(1)(ii)(A) - Risk Analysis

HIPAA - Security Rule	Other Requirements
164.308(a)(1)(ii)(A) Risk Analysis	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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 or business associate.

Guidance
This is the most common failure cited in most HIPAA penalties. By not conducting an accurate and thorough Security Risk Analysis, cybersecurity controls are not adequately implemented.

For medical providers, this is a requirement of the Medicare MIPS financial incentive program.

HIPAA Audit Protocol:

Does the entity have policies and procedures in place to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creates, receives, maintains, or transmits?

Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits?

Determine how the entity has implemented the requirements.

Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated.

Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. Evaluate and determine whether the risk analysis or other documentation contains:
• A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI
• Details of identified threats and vulnerabilities
• Assessment of current security measures
• Impact and likelihood analysis
• Risk rating

Obtain and review documentation regarding the written risk analysis or other documentation that immediately preceded the current risk analysis or other record, if any. Evaluate and determine if the risk analysis has been reviewed and updated on a periodic basis, in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event.

If there is no prior risk analysis or other record, obtain and review the two (2) most recent written updates to the risk analysis or other record, if any. If the original written risk analysis or other records have not been updated since they were originally conducted and/or drafted, obtain and review an explanation as to the reason why.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CC1.1 - Inventories: Establish and maintain inventories of organizational systems (including hardware, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.
- CC1.2 - Data Locations: Locate and identify all organizational data, including data stored on local devices, mobile devices, servers, mass storage, portable media, and cloud platforms.
- CC1.3 - Data Flow Mapping: Create a map of how data flows within and in/out of the organization.
- CC5.1 - Risk Assessment/Risk Analysis: Periodically conduct an accurate and thorough assessment of the risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of data.
- CC5.2 - Prioritize Risks: Prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.
- CC5.4 - End-of-Life Products: Manage products no longer supported by a vendor (e.g., end of life) separately and restrict as necessary to reduce risk.
- CC14.6 - Critical Functions: Identify all critical functions.
- CC14.7 - Dependencies: Identify and document all dependencies for each critical function. Include technology, people, and facilities.
- CC14.8 - Resiliency Requirements: Establish resilience requirements to support the delivery of critical services.
- CC14.9 - Business Impact Analysis: Conduct Business Impact Analyses (BIA) with all departments to measure the financial, regulatory, and reputational impact of incidents.
- CC14.10 - Likelihood Analysis: Determine the likelihood of an incident based on historical information and other resources.
- CC14.11 - Alternative Processes: Identify alternative processes for all critical functions.
- CC17.1 - Vulnerability Scans: Scan for vulnerabilities and encryption status in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
- CC17.2 - Vulnerability Plan: Ensure that a written vulnerability management plan is developed and implemented.
- CC17.7 - Risk Determination: Determine risk using threats, vulnerabilities, likelihoods, and impacts.
- CC17.10 - Risk Tolerance: Organization risk tolerance is determined and clearly expressed.
- CC17.12 - Newly-Identified Vulnerabilities: Ensure that newly identified vulnerabilities are mitigated or documented as accepted risks.

References

- HIPAA Security Rule Administrative Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
- Guidance on Risk Analysis - https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es

HIPAA 164.308(a)(1)(ii)(B) - Risk Management

HIPAA - Security Rule	Other Requirements
164.308(a)(1)(ii)(B) Risk Management	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Guidance
Risk management is the process used to identify and implement security measures to reduce risk to a reasonable and appropriate level within the covered entity based on the covered entity's circumstances.

HIPAA Audit Protocol:

Does the entity have policies and procedures in place regarding a risk management process sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level?

Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level?

Obtain and review policies and procedure related to risk management. Evaluate and determine if the documents identify how risk will be managed, what is considered an acceptable level of risk based on management approval, the frequency of reviewing ongoing risks, and identify workforce members' roles in the risk management process.

Obtain and review documentation demonstrating the security measures implemented and/or in the process of being implemented as a result of the risk analysis or assessment. Evaluate and determine whether the implemented security measures appropriately respond to the threats and vulnerabilities identified in the risk analysis according to the risk rating and that such security measures are sufficient to mitigate or remediate identified risks to an acceptable level.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC1.4 - Data Flow Management: Ensure that a baseline of network operations and expected data flows for users and systems is established and managed.
- CC3.2 - Governance & Risk Management Processes: Ensure governance and risk management processes address cybersecurity risks.
- CC5.3 - Risk Management/Mitigation: Implement security measures sufficient to mitigate or reduce risks and vulnerabilities to a reasonable and appropriate level.

- CC8.1 - Protect Data: Ensure data-at-rest (stored) is protected.
- CC8.2 - Manage Assets: Ensure assets are formally managed throughout removal, transfers, and disposition.
- CC17.3 - Manage Vulnerabilities: Remediate vulnerabilities in accordance with risk assessments.
- CC17.11 - Risk Tolerance Alignment: Risk management aligns with all legal and regulatory requirements, the organization's role in critical infrastructure, and a sector-specific risk analysis.

References

- HIPAA Security Rule Administrative Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
- Risk Analysis & Risk Management - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf?language=es

HIPAA 164.308(a)(1)(ii)(C) - Sanction Policy

HIPAA - Security Rule	Other Requirements
164.308(a)(1)(ii)(C) Sanction Policy	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

Guidance
Appropriate sanctions must be in place so that workforce members understand the consequences of failing to comply with security policies and procedures, to deter noncompliance.

HIPAA Audit Protocol:

Does the entity have policies and procedures in place regarding sanctions to apply to workforce members who fail to comply with the entity's security policies and procedures?

Does the entity apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures?

Obtain and review documentation of the sanction policies and procedures (which could be an aspect of a larger code of conduct). Evaluate if they contain a reasonable and appropriate process to sanction workforce members for failures to comply with the entity's security policies and procedures.

Elements to review may include but are not limited to:
• Personnel involved in the sanction process
• Required steps and time period
• Notification steps
• Reason for the sanction
• Identification of the sanctions applied to compliance failures
• Documentation of the sanction outcome

Obtain and review documentation demonstrating sanctions against workforce members. Evaluate and determine whether appropriate sanctions were applied for workforce members that failed to comply with security policies and procedures.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC4.1 - Written Cybersecurity Policies: Write policies addressing all cybersecurity requirements.

- CC4.2 - Written Compliance Policies: Write policies addressing all compliance requirements.
- CC4.3 - Written Procedures: Create written documentation for each procedure.
- CC4.5 - Sanction Policy: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures.

References

- HIPAA Security Rule Administrative Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review

HIPAA - Security Rule	Other Requirements
164.308(a)(1)(ii)(D) Information System Activity Review	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Guidance
This is the first of several related requirements for logging activities related to Protected Health Information (PHI). Related requirements include Audit Controls (logging all PHI-related activity) and Unique User Identification.

HIPAA Audit Protocol:

Does the entity have policies and procedures in place regarding the regular review of information system activity?

Does the entity regularly review records of information system activity?

Obtain and review policies and procedures related to reviewing records of information system activities. Evaluate and determine if reasonable and appropriate processes are in place to review records of information system activities, such as audit logs, access reports, and security incident tracking reports.

Elements to review may include but are not limited to:
• How often a review is performed
• How reviews are documented
• Workforce members' roles and responsibilities in the regular records of the information systems activities
• Types of activities which may require further investigation

Obtain and review documentation demonstrating the records of information system activities that were reviewed such as audit logs, access reports, and security incident tracking reports. Evaluate and determine if information system records were reviewed in a timely manner and that the review was conducted and certified by appropriate personnel.

Obtain and review documentation demonstrating the capabilities of the information system activity logs. Evaluate and determine whether key information systems have the capabilities to generate activity records; and, if so, are the capabilities turned on and records generated.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CC10.3 - Review Log Records: Ensure that audit/log records are reviewed regularly to identify unusual or unauthorized activity.

References

- HIPAA Security Rule Administrative Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA 164.308(a)(2) - Assigned Security Responsibility

HIPAA - Security Rule	Other Requirements
164.308(a)(2) Assigned Security Responsibility	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity.

Guidance
Typically this is the person in charge of IT security. The responsibility can also be assigned to the HIPAA Compliance Officer.

HIPAA Audit Protocol:

Does the entity have policies and procedures in place regarding the establishment of a security official?

Has the entity identified the security official responsible for the development and implementation of the policies and procedures required by this subpart?

Obtain and review documentation of the assigned Security Official(s) responsibilities (e.g., job description) and that a natural person has been named to act as the Security Official and/or other individuals have been assigned with other security duties. Evaluate and determine whether the organization has assigned responsibility for compliance with the Security Rule to a Security Official who oversees the development and implementation (to include monitoring and communication) of security policies and procedures and/or assigned other individuals with other security duties; and the responsibilities of the Security Official(s) have been clearly defined.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC2.3 - Security Official: Identify the security official who is responsible for the development and implementation of the security policies and procedures.

References
- HIPAA Security Rule Administrative Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA 164.308(a)(3)(ii)(A) - Authorization and/or Supervision

HIPAA - Security Rule	Other Requirements
164.308(a)(3)(ii)(A) Authorization and/or Supervision	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Guidance
Access authorization is the process where a department head or HR verifies to the IT department or software administrator that a user is entitled to access.

HIPAA Audit Protocol:

Does the entity have policies and procedures in place regarding the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed?

Does the entity authorize and/or supervise workforce member who work with ePHI or in locations where it might be accessed?

Obtain and review policies and procedures related to the authorization and/or supervision of workforce members. Evaluate the content in relation to the specified performance criteria and determine that appropriate authorization and/or supervision of workforce members who work with ePHI or in a location where it might be accessed is incorporated in the process.

Obtain and review documentation regarding how requests for information systems that contain ePHI and access to ePHI are processed. Evaluate and determine if appropriate authorization and/or supervision for granting access to information systems that contain ePHI is incorporated in the process and is in accordance with related policies and procedures.

Elements to review may include but are not limited to:
• Identification of who has the authorization and/or supervisory permission to approve access to information systems and/or locations where ePHI may be accessed
• How access requests to information systems are submitted
• How access to the information systems is granted
• How requests to access ePHI are submitted
• How access to ePHI is granted
• How authorization and/or supervisory approvals are verified
• How a workforce member's level of access to ePHI is verified

Obtain and review documentation demonstrating how access requests to locations where ePHI might be accessed are processed. Evaluate and determine if appropriate authorization for granting access to locations where ePHI might be accessed is incorporated in the process and is in accordance with related policies and procedures.

Elements to review may include but are not limited to:
• How access requests to locations are submitted
• How access requests to locations are granted
• How authorization and/or supervisory approvals are verified
• How a workforce member's level of access to a location is verified

Obtain and review documentation of workforce members who were authorized access to ePHI or locations where ePHI might be accessed and organizational charts/lines of authority. Evaluate and determine if access requests were properly authorized in accordance with the entity's related policies and procedures and in accordance with established lines of authority.

Has the entity chosen to implement an alternative measure?

If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.

Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC2.4 - Workforce Cybersecurity Roles & Responsibilities: Establish and document cybersecurity roles and responsibilities within the workforce.
- CC2.5 - Third-Party Cybersecurity Roles & Responsibilities: Establish and document cybersecurity roles and responsibilities with third-party stakeholders.
- CC2.6 - Workforce Compliance Roles & Responsibilities: Establish compliance roles and responsibilities within the workforce.
- CC2.7 - Third-Party Compliance Roles & Responsibilities: Establish compliance roles and responsibilities with third-party stakeholders.
- CC6.1 - Screen Individuals: Screen individuals prior to authorizing access to organizational systems.
- CC7.25 - Authorize Wireless Access: Authorize wireless access prior to allowing such connections.
- CC7.34 - Authorize Privileged Remote Sessions: Authorize remote execution of privileged commands and remote access to security-relevant information.

References
- HIPAA Security Rule Administrative Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA 164.308(a)(3)(ii)(B) - Workforce Clearance Procedure

HIPAA - Security Rule	Other Requirements
164.308(a)(3)(ii)(B) Workforce Clearance Procedure	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

Guidance
Procedures may include criminal background checks, verification of licenses, credentialing, credit checks, and checking references and past employment history.

HIPAA Audit Protocol:

Does the entity have policies and procedures in place to determine that a workforce member's access to ePHI is appropriate?

Does the entity determine whether a workforce member's access to ePHI is appropriate?

Obtain and review documentation related to workforce clearance procedures. Evaluate and determine whether such procedures has been incorporated to determine whether a workforce member's access to ePHI is appropriate.

Elements to review may include but are not limited to:
• Clearing workforce members prior to authorizing access to ePHI
• Revalidation of workforce members' clearance
• Frequency of revalidating workforce members' clearance.

Obtain and review documentation demonstrating the clearance process prior to granting workforce members access to ePHI. Obtain and review documentation demonstrating approval or verification of access to ePHI (e.g., approved access request forms, electronic approval workflow, etc.). Evaluate and determine if workforce members were granted appropriate access to ePHI based on the clearance process prior to gaining access to ePHI.

Has the entity chosen to implement an alternative measure?
If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.
Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC6.1 - Screen Individuals: Screen individuals prior to authorizing access to organizational systems.

References
- HIPAA Security Rule Administrative Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

Truncated Sample Report