

HIPAA Security Standards Final Rule

CMS - Office of
HIPAA Standards
(OHS)

Regulation Dates

- Published February 20, 2003
- Effective Date April 21, 2003

- Compliance Date:
 - April 21, 2005 for all covered entities except small health plans
 - April 21, 2006 for small health plans (as HIPAA requires)

General Requirements - 164.306(a)

■ Ensure

- Confidentiality (only the right people see it)
- Integrity (the information is what it is supposed to be – no unauthorized alteration or destruction)
- Availability (the right people can see it when needed)

General Requirements

- Applies to Electronic Protected Health Information (PHI)
- That a Covered Entity Creates, Receives, Maintains, or Transmits

General Requirements

- Protect against reasonably anticipated threats or hazards to the security or integrity of information
- Protect against reasonably anticipated uses and disclosures not permitted by privacy rules
- Ensure compliance by workforce

Regulation Themes

- Scalability/Flexibility
 - Covered entities can take into account:
 - Size
 - Complexity
 - Capabilities
 - Technical Infrastructure
 - Cost of procedures to comply
 - Potential security risks

Regulation Themes

- Technologically Neutral
 - What needs to be done, not how
- Comprehensive
 - Not just technical aspects, but behavioral as well

How Is This Accomplished

- Standards Are Required but:
 - Implementation specifications which provide more detail can be either required or addressable.

Addressability

- If an implementation specification is addressable, a covered entity can:
 - Implement, if reasonable and appropriate
 - Implement an equivalent measure, if reasonable and appropriate
 - Not implement it
- Based on sound, documented reasoning from a risk analysis

Maintenance

- Implemented security measures for compliance must be reviewed and modified as needed to continue reasonable and appropriate protections

What are the Standards?

- Five Sections:
 - 164.308: Administrative Safeguards
 - 164.310: Physical Safeguards
 - 164.312: Technical Safeguards
 - 164.314: Organizational Requirements
 - 164.316: Policies and Procedures and Documentation Requirements

Administrative Safeguards

§164.308

Standards and
Implementation
Specifications

Administrative Safeguards

- 164.308(a)(1)(i) Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations
 - (ii)(A) Risk Analysis (R)
 - (ii)(B) Risk Management (R)
 - (ii)(C) Sanction Policy (R)
 - (ii)(D) Information System Activity Review (R)

Administrative Safeguards

- 164.308(a)(2) Assigned Security Responsibility (R): Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity

Administrative Safeguards

- 164.308(a)(3)(i) Workforce Security:
Implement policies and procedures to ensure that all workforce members have appropriate access and to prevent workforce members without access from obtaining access [to electronic PHI as provided in Information Access Management]
 - (ii)(A) Authorization and/or Supervision (A)
 - (ii)(B) Workforce Clearance Procedure (A)
 - (ii)(C) Termination Procedures (A)

Administrative Safeguards

- 164.308(a)(4)(i) Information Access Management: Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of [the Privacy Rule]
 - (ii)(A) Isolating Health Care Clearinghouse Functions (R)
 - (ii)(B) Access Authorization (A)
 - (ii)(C) Access Establishment and Modification (A)

Administrative Safeguards

- 164.308(a)(5)(i) Security Awareness and Training: Implement a security awareness and training program for all workforce members (including management)
 - (ii)(A) Security Reminders (A)
 - (ii)(B) Protection from Malicious Software (A)
 - (ii)(C) Log-in Monitoring (A)
 - (ii)(D) Password Management (A)

Administrative Safeguards

- 164.308(a)(6)(i) Security Incident Procedures: Implement policies and procedures to address security incidents
 - (ii) Response and Reporting (R)

Administrative Safeguards

- 164.308(a)(7)(i) Contingency Plan:
Establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic PHI
 - (ii)(A) Data Backup Plan (R)
 - (ii)(B) Disaster Recovery Plan (R)
 - (ii)(C) Emergency Mode Operation Plan (R)
 - (ii)(D) Testing and Revision Procedures (A)
 - (ii)(E) Applications and Data Criticality Analysis (A)

Administrative Safeguards

- 164.308(a)(8) Evaluation (R): Perform a periodic technical and nontechnical evaluation...that establishes the extent to which an entity's security policies and procedures meet the [Security Rule requirements]
 - Initially upon the standards implemented under this rule;
 - Subsequently, in response to environmental or operational changes affecting the security of electronic PHI

Administrative Safeguards

- 164.308(b)(1) Business Associate Contracts and Other Arrangements: A covered entity [CE] may permit a business associate [BA] to create, receive, maintain, or transmit electronic PHI on the [CE's] behalf only if the [CE] obtains satisfactory assurances that the [BA] will appropriately safeguard the information
 - (b)(4) Written Contract or Other Arrangement (R)

Physical Safeguards

§164.310

Standards and
Implementation
Specifications

Physical Safeguards

- 164.310(a)(1) Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed
 - (2)(i) Contingency Operations (A)
 - (2)(ii) Facility Security Plan (A)
 - (2)(iii) Access Control and Validation Procedures (A)
 - (2)(iv) Maintenance Records (A)

Physical Safeguards

- 164.310(b) Workstation Use (R): Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI

Physical Safeguards

- 164.310(c) Workstation Security (R): Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users

Physical Safeguards

- 164.310(d)(1) Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility
 - (2)(i) Disposal (R)
 - (2)(ii) Media Re-use (R)
 - (2)(iii) Accountability (A)
 - (2)(iv) Data Backup and Storage (A)

Technical Safeguards

§164.312

Standards and
Implementation
Specifications

Technical Safeguards

- 164.312(a)(1) Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in... [Information Access Management]
 - (2)(i) Unique User Identification (R)
 - (2)(ii) Emergency Access Procedure (R)
 - (2)(iii) Automatic Logoff (A)
 - (2)(iv) Encryption and Decryption (A)

Technical Safeguards

- 164.312(b) Audit Controls (R): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI

Technical Safeguards

- 164.312(c)(1) Integrity: Implement policies and procedures to protect electronic PHI from improper alteration or destruction
 - (c)(2) Mechanism to authenticate electronic PHI (A)

Technical Safeguards

- 164.312(d) Person or Entity Authentication (R): Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed

Technical Safeguards

- 164.312(e)(1) Transmission Security: Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network
 - (2)(i) Integrity Controls (A)
 - (2)(ii) Encryption (A)

Organizational Requirements

§164.314

Standards and
Implementation
Specifications

Organizational Requirements

- 164.314(a)(1) Business Associate Contracts or Other Arrangements
 - (2)(i) Business Associate Contracts (R): Contract between a covered entity and a business associate
 - (2)(ii) Other Arrangements (R): Covered entity and its business associate are both governmental entities

Organizational Requirements

- 164.314(b)(1) Requirements for Group Health Plans: Ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic PHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan
 - (b)(2) Plan Documents (R)

Policies and Procedures and Documentation

§164.314

Standards and
Implementation
Specifications

Policies and Procedures and Documentation

- 164.316(a) Policies and Procedures (R): Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of [the Security Rule], taking into account [General Rules - §164.306(b)(2)(i)-(iv)]

Policies and Procedures and Documentation

- 164.316(b)(1) Documentation:
Maintain policies, and procedures, [and] actions, activities or assessments implemented to comply with the standards, in written (which may be electronic) form
 - (2)(i) Time Limit (R)
 - (2)(ii) Availability (R)
 - (2)(iii) Updates (R)

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Security Plan (R)
Assigned Security Responsibilities	164.308(a)(2)	Authorization and/or Supervision (R) Workforce Clearance Procedure Termination Procedures (A)
Workforce Security	164.308(a)(3)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A) Access Termination (A) Protection from Internal Security (R) Log-in Monitoring (A) Password Management (A)
Information Access Management	164.308(a)(4)	Disaster Recovery Plan (R) Emergency Mode Operations (R) Continuity of Operations (R) Application of Security Standards (R)
Security Awareness and Training	164.308(a)(5)	Written Contract or Other Arrangement (R)
Security Incident Response	164.308(a)(6)	
Security Evaluation	164.308(a)(7)	
Business Associate Contracts and Other Arrangements	164.308(b)(1)	
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

Appendix A in Regulation

- End of regulation, chart lists each standard, its associated implementation specifications, and if required or addressable

Implementation Approach

- Do Risk Analysis – Document
- Based on Risk Analysis, determine how to implement each standard and implementation specification – Document
- Develop Security Policies and Procedures – Document
- Train Workforce
- Implement Policies and Procedures
- Periodic Evaluation

Summary

- Scalable, flexible, technology neutral approach
- First step is risk analysis
- Standards that make good business sense
- Provided two year implementation

CMS/OHS HIPAA Resources

- <http://www.cms.hhs.gov/hipaa/hipaa2/> - CMS HIPAA Administrative Simplification Website for Electronic Transactions and Code Sets, Security, and Unique Identifiers
- <https://htct.hhs.gov/> - Administrative Simplification Enforcement Tool (ASET) HIPAA Transactions and Code Sets Complaint System