

Guide to Final Security Rule

164 SECURITY AND PRIVACY

164.103 Definitions.

164.104 Applicability.

164.105 Organizational requirements.

Subpart C – Security Standards for the Protection of Electronic Protected Health Information

164.302 Applicability.

164.304 Definitions.

164.306 Security standards: General rules.

- (a) *General requirements.*
 - (1) confidentiality, integrity, and availability of electronic PHI
 - (2) threats or hazards
 - (3) uses or disclosures not permitted or required
 - (4) workforce compliance
- (b) *Flexibility of approach.*
 - (1) reasonably and appropriately implement standards and implementation specifications
 - (2) factors:
 - (i) size, complexity, capabilities
 - (ii) technical infrastructure, hardware, software security capabilities
 - (iii) costs
 - (iv) probability and criticality of risks
- (c) *Standards.*
- (d) *Implementation specifications.*
 - (1) required or addressable
 - (2) required implementation specifications
 - (3) addressable implementation specifications
 - (i) assess whether reasonable and appropriate safeguard
 - (ii) as applicable
 - (A) implement
 - (B) if not reasonable and appropriate
 - (1) document
 - (2) implement equivalent alternative
- (e) *Maintenance.*

164.308 Administrative safeguards.

- (a) covered entity must
 - (1) (i) *Standard: Security management process.*
 - (ii) *Implementation specifications:*
 - (A) *Risk analysis* (Required).
 - (B) *Risk management* (Required).
 - (C) *Sanction policy* (Required).
 - (D) *Information system activity review* (Required).
 - (2) *Standard: Assigned security responsibility.*
 - (3) (i) *Standard: Workforce security.*
 - (ii) *Implementation specifications:*

- (A) *Authorization and/or supervision* (Addressable).
- (B) *Workforce clearance procedure* (Addressable).
- (C) *Termination procedures* (Addressable).
- (4) (i) *Standard: Information access management.*
- (ii) *Implementation specifications:*
 - (A) *Isolating health care clearinghouse functions* (Required).
 - (B) *Access authorization* (Addressable).
 - (C) *Access establishment and modification* (Addressable).
- (5) (i) *Standard: Security awareness and training.*
- (ii) *Implementation specifications:*
 - (A) *Security reminders* (Addressable).
 - (B) *Protection from malicious software* (Addressable).
 - (C) *Log-in monitoring* (Addressable).
 - (D) *Password management* (Addressable).
- (6) (i) *Standard: Security incident procedures.*
- (ii) *Implementation specification: Response and Reporting* (Required)
- (7) (i) *Standard: Contingency plan.*
- (ii) *Implementation specifications:*
 - (A) *Data backup plan* (Required).
 - (B) *Disaster recovery plan* (Required).
 - (C) *Emergency mode operation plan* (Required).
 - (D) *Testing and revision procedures* (Addressable).
 - (E) *Applications and data criticality analysis* (Addressable).
- (8) *Standard: Evaluation.*
- (b) (1) *Standard: Business associate contracts and other arrangements.*
- (2) does not apply with respect to --
 - (i) transmission of electronic PHI to health care provider concerning treatment
 - (ii) transmission of electronic PHI by group health plan or HMO to plan sponsor
 - (iii) transmission of electronic PHI from or to other agencies when CE is health plan that is government program providing public benefits
- (3) noncompliance
- (4) *Implementation specifications: Written contract or other arrangement* (Required).

164.310 Physical safeguards.

A covered entity must:

- (a) (1) *Standard: Facility access controls.*
- (2) *Implementation specifications:*
 - (i) *Contingency operations* (Addressable).
 - (ii) *Facility security plan* (Addressable).
 - (iii) *Access control and validation procedures* (Addressable).
 - (iv) *Maintenance records* (Addressable).
- (b) *Standard: Workstation use.*
- (c) *Standard: Workstation security.*
- (d) (1) *Standard: Device and media controls.*
- (2) *Implementation specifications:*
 - (i) *Disposal* (Required).
 - (ii) *Media re-use* (Required).
 - (iii) *Accountability* (Addressable).
 - (iv) *Data backup and storage* (Addressable).

164.312 Technical safeguards.

A covered entity must:

- (a) (1) *Standard: Access control.*

- (2) *Implementation specifications:*
 - (i) *Unique user identification* (Required).
 - (ii) *Emergency access procedure* (Required).
 - (iii) *Automatic logoff* (Addressable).
 - (iv) *Encryption and decryption* (Addressable).
- (b) *Standard: Audit controls.*
- (c) (1) *Standard: Integrity.*
- (2) *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable).
- (d) *Standard: Person or entity authentication.*
- (e) (1) *Standard: Transmission security.*
- (2) *Implementation specifications:*
 - (i) *Integrity controls* (Addressable).
 - (ii) *Encryption* (Addressable).

164.314 Organizational requirements.

- (a) (1) *Standard: Business associate contracts or other arrangements.*
 - (i) meet requirements of (a)(2)(i) or (a)(2)(ii) as applicable
 - (ii) business associate material breach or violation
 - (A) terminate contract if feasible
 - (B) report to the Secretary
- (2) *Implementation specifications* (Required).
 - (i) *Business associate contracts*
 - (A) administrative, physical, technical safeguards
 - (B) agent safeguards
 - (C) report security incidents
 - (D) authorize termination of contract
 - (ii) *Other arrangements.*
 - (A) governmental entities
 - (1) memorandum of understanding
 - (2) other law
 - (B) legal mandate
 - (C) statutory obligations
- (b) (1) *Standard: Requirements for group health plans*
- (2) *Implementation specifications* (Required).
 - (i) administrative, physical, technical safeguards
 - (ii) adequate separation
 - (iii) agent security measures
 - (iv) report security incidents

164.316 Policies and procedures and documentation requirements.

- A covered entity must:
- (a) *Standard: Policies and procedures.*
 - (b) (1) *Standard: Documentation.*
 - (i) maintain
 - (ii) written record of action, activity, assessment
 - (2) *Implementation specifications:*
 - (i) *Time limit* (Required).
 - (ii) *Availability* (Required).
 - (iii) *Updates* (Required).

164.318 Compliance dates for the initial implementation of the security standards.

- (a) *Health plan.*
 - (1) not a small health plan April 20, 2005
 - (2) small health plan April 20, 2006
- (b) *Health care clearinghouse.* April 20, 2005

(c) *Health care provider.*

April 20, 2005