

Summary of the Final HIPAA Security Rules

February 20 2003

164.306 Security Standards: General Rules

(a) General requirements.

Covered entities (CE) must do the following :

- (1) Ensure confidentiality, integrity, and availability (CIA) of all electronic protected health information (EPHI) the CE creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to EPHI.
- (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- (4) Ensure compliance with this subpart by its workforce.

(b) Flexibility of approach.

- (1) CE may use any security measures that allow the CE to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
- (2) In deciding which security measures to use, a CE must take into account the following factors:
 - (i) the size, complexity, and capabilities of the covered entity,
 - (ii) the CE's technical infrastructure, hardware, and software security capabilities,
 - (iii) the cost of security measures, and
 - (iv) the probability and criticality of potential risks to EPHI.

(c) Standards.

A CE must comply with the standards as provided in this section and in sections 164.308, 164.310, 164.312, 164.314, and 164.316 with respect to all EPHI.

(d) Implementation specifications.

- (1) Implementation specifications are either required (**R**) or addressable.
- (2) Required standards **MUST** be implemented by the CE.
- (1) For addressable standards, CE's must:
 - (i) assess whether a standard is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the CE's EPHI and
 - (ii) As applicable to the entity --
 - (A) implement the specification if reasonable and appropriate, or
 - (B) if implementation specification is not, reasonable and appropriate
 - (1) document why it would not be reasonable and appropriate to implement and
 - (2) implement an equivalent alternative measure if reasonable and appropriate.

(e) Maintenance.

Security measures implemented to comply with standards and implementation specifications adopted under 165.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of EPHI as described in 164.316.

164.308 Administrative safeguards

(a)

- (1)(i) Security management process
Implement policies and procedures to prevent, detect, contain, and correct security violations.
- (ii) Implementation Specifications:
 - (A) **Risk analysis (R)** - **Conduct** (refer to deans/chairmen/directors) an **accurate and thorough assessment of potential risks** and vulnerabilities to CIA of EPHI.
 - (B) **Risk Mgmt. (R)** - **Implement security measures sufficient to reduce risks** and vulnerabilities to a reasonable and appropriate level to comply with 164.306.
 - (C) **Sanction policy (R)** - **(Specify and) Apply appropriate sanctions** against workforce members who fail to comply with the security policies and procedures.
 - (D) **Information (R)** - Implement **procedures to regularly review** records of IS activity sys. activity review (i.e. audit logs, access reports, security incident tracking reports).
- (2) **Assigned security responsibility (R)**
- (3)(i) Workforce security
Implement policies and procedures to ensure that all **workforce members have appropriate access** to EPHI as provided under paragraph (a)(4) of this section, and to **prevent those members who do not have access** under (a)(4) from obtaining access to EPHI.
- (ii) Implementation Specifications:
 - (A) Authorization and/ or supervision - **Implement procedures for the authorization/supervision of** workforce members who work with EPHI or in locations where it might be accessed.
 - (B) Workforce clearance- Implement **procedures to determine** that the **access** of a procedure workforce member to EPHI is **appropriate**.
 - (C) **Termination Procedures** - Implement **procedures for terminating staff access to EPHI** (i.e. end of employment, determination as in section (a) 3.B.)
- (4)(i) Information access management
Implement policies and procedures for authorizing access to EPHI consistent with subpart E
- (ii) Implementation Specifications:
 - (A) **Isolate health care clearinghouse fcns (R)** -If clearinghouse part of larger organization, the clearinghouse must implement policies and procedures that protect EPHI from unauthorized access by the larger organization.
 - (B) Access authorization - Implement **policies and procedures for granting access to EPHI** (i.e. thru workstation, transaction, program, process, etc.).
 - (C) Access establishment and modification - Implement **policies and procedures that** , based on 4.B, **establish, document, review, and modify user's right of access to a workstation, transaction, program or process**.
- (5)(i) Security awareness and training.
Implement a security awareness and training program for all members of the workforce including management.
- (ii) Implementation Specifications:
 - (A) Security reminders - Implement periodic security updates.
 - (B) Protection from malicious software - **Implement procedures for guarding against, detecting, and reporting malicious software**.
 - (C) Log-in monitoring - Implement **procedures for monitoring log-in attempts and reporting discrepancies**.

(D) Password mgmt. - Implement *procedures for creating, changing, and safeguarding passwords.*

(6)(i) Security incident procedures

Implement *policies and procedures to address security incidents.*

(ii) Implementation Specifications:

- Response and Reporting (R)**
- Identify and respond to suspected or known security incidents.
 - Mitigate to the extent practicable, harmful effects of security incidents that are known to the CE.
 - Document security incidents and their outcomes.

(7)(i) Contingency plan

Establish *policies and procedures for responding to an emergency or other occurrence (fire, vandalism, system failure, natural disaster, etc.) that damages systems that contain electronic protected health information.*

(ii) Implementation Specifications:

- (A) **Data backup plan (R)** - Establish/implement *procedures to create and maintain retrievable exact copies of EPHI.*
- (B) **Disaster recovery plan (R)** - Establish/implement *procedures to restore any loss of data.*
- (C) **Emergency mode operation plan (R)** - Establish/implement *procedures to enable continuation of critical business processes for the protection of the security if EPHI while operating in emergency mode.*
- (D) Testing and revision - implement *procedures for periodic testing and revision of contingency plans.*
- (E) Applications and data criticality analysis - Access the relative criticality of specific applications and data in support of other contingency plan components

(8)(i) Evaluation (R)

Perform a periodic technical and non-technical evaluation, based initially upon standards but subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity's security policies and procedures meet the requirement of this subpart.

(b)

(1) Business associate (BA) contracts and other arrangements

A CE, in accordance with 164.314(a), may permit a BA to create, receive, maintain, or transmit EPHI information on the CE's behalf only if the CE obtains satisfactory assurances in accordance with 164.314(a) that the BA will properly safeguard the information.

(2) This standard does not apply with respect to -

- (i) The transmission of a CE of EPHI to a health care provider concerning the treatment of an individual.
- (ii) The transmission of EPHI by a group health plan or HMO, etc.
- (iii) The transmission of EPHI from or to other agencies providing the services at 164.502(e)(1)(ii)(C), when the CE is a health plan that is a government program providing public benefits, if the requirements of 164.502(e)(1)(ii)(C) are met.

(3) A CE that violates the satisfactory assurances it provided as a BA of another CE will be in non compliance with the standards, and requirements of this paragraph and 164.314(a).

(4) Implementation specification:

- Written contract or other arrangement (R)** - Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with BA that meets the applicable requirements of 164.314(a).

164.310 Physical Safeguards

A CE must , in accordance with 164.306:

(a)

(1) Facility access controls

Implement *policies and procedures*:

to *limit physical access* to electronic information systems,
to *limit access to the facilities* in which they are housed, and

to *ensure* that *properly authorized access* is allowed.

(2) Implementation specifications:

(i) Contingency operations

Establish (and implement as necessary) *procedures that allow facility access in support of: restoration of lost data* under the disaster recovery plan and *emergency mode operations plan* in the event of an emergency.

(ii) Facility security plan

Implement *policies and procedures to safeguard the facility and the equipment therein* from unauthorized physical access, tampering, and theft.

(iii) Access control and validation procedures

Implement *procedures to control and validate a person's access to facilities* based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) Maintenance records

Implement *policies and procedures to document repairs and modifications* to the physical components of a facility which are related to security (i.e. doors, locks, walls, hardware, etc.)

(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 EPHI.

(c)

Workstation security (R)

Implement physical safeguards for all workstations that access EPHI to *restrict access to authorized users*.

(d)

(1) Device and media controls

Implement *policies and procedures* that *govern* the *receipt and removal of hardware and electronic media* that contain EPHI into and out of a facility, and the movement of these items within the facility.

(2) Implementation specifications

(i) Disposal (R)

Implement *policies and procedures* to *address* the *final disposition* of *EPHI* and/or the *hardware* or electronic *media* on which it is stored.

(ii) Media re-use (R)

Implement *procedures for the removal of EPHI from electronic media* before the media are made available for re-use.

(iii) Accountability

Maintain a record of the movements of hardware and electronic *media* and any person responsible for it.

(iv) Data backup and storage

Create a retrievable, *exact copy* of EPHI when needed *before the movement of equipment*.

164.312 Technical safeguards

A CE must in accordance with 164.306:

(a)

(1) Access control

Implement technical *policies and procedures* for electronic information systems that maintain EPHI to *allow access only to* those *persons* or software *programs* that have been *granted access rights* as specified in 164.308(a)(4)].

(2) Implementation specifications

(i) **Unique user identification (R)**

Assign a unique name and/or number for identifying and tracking user identity.

(ii) **Emergency access procedure (R)**

Establish (and implement as needed) *procedures for obtaining* necessary *EPHI during an emergency*.

(iii) Automatic logoff

Implement electronic *procedures* that terminate an *electronic session after a predetermined time* of inactivity.

(iv) Encryption and decryption

Implement a mechanism to encrypt and decrypt EPHI.

(b)

Audit controls (R)

Implement hardware, software, and/or procedural *mechanisms* that *record and examine activity* in information systems that contain or use EPHI.

(c)

(1) Integrity

Implement *policies and procedures to protect* EPHI from *improper alteration or destruction*.

(2) Mechanism to authenticate EPHI

Implement electronic mechanisms to corroborate that *EPHI* has *not* been *altered or destroyed in an unauthorized manner*.

(d)

Person or entity authentication (R)

Implement *procedures to verify* that a *person or entity* seeking access to EPHI is *the one claimed*.

(e)

(1) Transmission security

Implement *technical* security *measures* to *guard against* unauthorized *access* to EPHI that is *being transmitted* over an electronic communications network.

(2) Implementation specifications

(i) Integrity controls

Implement *security measures* to ensure that electronically *transmitted EPHI* is *not improperly modified without detection* until disposed of.

(ii) Encryption

Implement a mechanism to *encrypt EPHI whenever deemed appropriate*.