

§ 164.306

§ 164.306 Security standards: General rules.

(a) *General requirements.* Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(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) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c) *Standards.* A covered entity must comply with the standards as provided in this section and in §164.308, §164.310, §164.312, §164.314, and §164.316 with respect to all electronic protected health information.

(d) *Implementation specifications.* In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes required implementa-

45 CFR Subtitle A (10-1-10 Edition)

tion specifications, a covered entity must implement the implementation specifications.

(3) When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes addressable implementation specifications, a covered entity must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and

(ii) As applicable to the entity—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

§(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.

(e) *Maintenance.* Security measures implemented to comply with standards and implementation specifications adopted under §164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at §164.316.

[68 FR 8376, Feb. 20, 2003; 68 FR 17153, Apr. 8, 2003]

§ 164.308 Administrative safeguards.

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

(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.

(2) *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

(3)(i) *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) *Implementation specifications*:

(A) *Authorization and/or supervision* (Addressable). 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.

(B) *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4)(i) *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) *Implementation specifications*:

(A) *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

(5)(i) *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

(ii) *Implementation specifications*. Implement:

(A) *Security reminders* (Addressable). Periodic security updates.

(B) *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(C) *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(D) *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

(6)(i) *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.

(ii) *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

(7)(i) *Standard: Contingency plan*. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for

§ 164.310

example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) *Implementation specifications:*

(A) *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) *Standard: Evaluation*. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

(b)(1) *Standard: Business associate contracts and other arrangements*. A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

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

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

45 CFR Subtitle A (10–1–10 Edition)

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of §164.314(b) and §164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at §164.502(e)(1)(ii)(C), when the covered entity 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 covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and §164.314(a).

(4) *Implementation specifications: Written contract or other arrangement* (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).

§ 164.310 Physical safeguards.

A covered entity must, in accordance with §164.306:

(a)(1) *Standard: 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) *Implementation specifications:*

(i) *Contingency operations* (Addressable). Establish (and implement as needed) 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* (Addressable). 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* (Addressable). Implement procedures to control and validate a person's access to facilities based on their