(e) *Maintenance*. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with §164.316(b)(2)(iii).

[68 FR 8376, Feb. 20, 2003; 68 FR 17153, Apr. 8, 2003; 78 FR 5693, Jan. 25, 2013]

§ 164.308 Administrative safeguards.

(a) A covered entity or business associate 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 or business associate.

(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 or business associate.

(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 covered entity or business associate.

(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, or other arrangement with, 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 covered entity's or the business associate'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 or business associate; 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 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 a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)(1) *Business associate contracts and other arrangements*. A covered entity 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. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.

(3) *Implementation specifications: Written contract or other arrangement (Required)*. Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§164.310 Physical safeguards.

A covered entity or business associate must, in accordance with §164.306:

(a)(1) *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its