

§ 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

(c)(1) *Standard: Documentation.* A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation as required by paragraph (c)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

#### § 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

[78 FR 5693, Jan. 25, 2013]

### Subpart B [Reserved]

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

AUTHORITY: 42 U.S.C. 1320d-2 and 1320d-4; sec. 13401, Pub. L. 111-5, 123 Stat. 260.

SOURCE: 68 FR 8376, Feb. 20, 2003, unless otherwise noted.

#### § 164.302 Applicability.

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

[78 FR 5693, Jan. 25, 2013]

#### § 164.304 Definitions.

As used in this subpart, the following terms have the following meanings:

*Access* means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to “access” as used in this subpart, not as used in subparts D or E of this part.)

*Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s or business associate’s workforce in relation to the protection of that information.

*Authentication* means the corroboration that a person is the one claimed.

*Availability* means the property that data or information is accessible and useable upon demand by an authorized person.

*Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.

*Encryption* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

*Facility* means the physical premises and the interior and exterior of a building(s).

*Information system* means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

*Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.

*Malicious software* means software, for example, a virus, designed to damage or disrupt a system.

*Password* means confidential authentication information composed of a string of characters.

*Physical safeguards* are physical measures, policies, and procedures to protect a covered entity’s or business associate’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

*Security or Security measures* encompass all of the administrative, physical, and technical safeguards in an information system.

*Security incident* means the attempted or successful unauthorized access, use,

## § 164.306

disclosure, modification, or destruction of information or interference with system operations in an information system.

*Technical safeguards* means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

*User* means a person or entity with authorized access.

*Workstation* means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

[68 FR 8376, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5693, Jan. 25, 2013]

### § 164.306 Security standards: General rules.

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

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate 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 and business associates may use any security measures that allow the covered entity or business associate 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 or business associate must take into account the following factors:

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

(ii) The covered entity's or the business associate's technical infrastruc-

## 45 CFR Subtitle A (10–1–13 Edition)

ture, 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 or business associate must comply with the applicable 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 implementation specifications, a covered entity or business associate 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 or business associate 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 electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

(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*. 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 sec-

tion, 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)(i)(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.

## § 164.310

(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.

## 45 CFR Subtitle A (10–1–13 Edition)

(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

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 role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) *Maintenance records (Addressable)*. Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) *Standard: Workstation use*. 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 protected health information.

(c) *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d)(1) *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) *Implementation specifications:*

(i) *Disposal (Required)*. Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hard-

ware or electronic media on which it is stored.

(ii) *Media re-use (Required)*. Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) *Accountability (Addressable)*. Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) *Data backup and storage (Addressable)*. Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

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

**§ 164.312 Technical safeguards.**

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

(a)(1) *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information 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 (Required)*. Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure (Required)*. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) *Automatic logoff (Addressable)*. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) *Encryption and decryption (Addressable)*. Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)(1) *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

**§ 164.314**

**45 CFR Subtitle A (10–1–13 Edition)**

(2) *Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).* Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication.* Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications:*

(i) *Integrity controls (Addressable).* Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

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

**§ 164.314 Organizational requirements.**

(a)(1) *Standard: Business associate contracts or other arrangements.* The contract or other arrangement required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) *Implementation specifications (Required).*

(i) *Business associate contracts.* The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes

aware, including breaches of unsecured protected health information as required by §164.410.

(ii) *Other arrangements.* The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3).

(iii) *Business associate contracts with subcontractors.* The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(b)(1) *Standard: Requirements for group health plans.* Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) *Implementation specifications (Required).* The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013; 78 FR 34266, June 7, 2013]

**§ 164.316 Policies and procedures and documentation requirements.**

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

(a) *Standard: Policies and procedures.* Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b)(1) *Standard: Documentation.* (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) *Implementation specifications:*

(i) *Time limit (Required).* Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability (Required).* Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) *Updates (Required).* Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5695, Jan. 25, 2013]

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

(a) *Health plan.* (1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) *Health care clearinghouse.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) *Health care provider.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

APPENDIX A TO SUBPART C OF PART 164—SECURITY STANDARDS: MATRIX

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
<b>Administrative Safeguards</b>		
Security Management Process .....	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R) (R)
Assigned Security Responsibility .....	164.308(a)(2)	Authorization and/or Supervision (A)
Workforce Security .....	164.308(a)(3)	Workforce Clearance Procedure Termination Procedures (A)
Information Access Management .....	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training .....	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)

§ 164.400

45 CFR Subtitle A (10–1–13 Edition)

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Security Incident Procedures .....	164.308(a)(6)	Response and Reporting (R) Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A) (R) Written Contract or Other Arrangement (R)
Contingency Plan .....	164.308(a)(7)	
Evaluation .....	164.308(a)(8)	Written Contract or Other Arrangement (R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	
<b>Physical Safeguards</b>		
Facility Access Controls .....	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A) (R) (R) Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Workstation Use .....	164.310(b)	
Workstation Security .....	164.310(c)	
Device and Media Controls .....	164.310(d)(1)	
<b>Technical Safeguards</b> (see § 164.312)		
Access Control .....	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A) (R) Mechanism to Authenticate Electronic Protected Health Information (A) (R) Integrity Controls (A) Encryption (A)
Audit Controls .....	164.312(b)	
Integrity .....	164.312(c)(1)	
Person or Entity Authentication .....	164.312(d)	
Transmission Security .....	164.312(e)(1)	

**Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information**

SOURCE: 74 FR 42767, Aug. 24, 2009, unless otherwise noted.

**§ 164.400 Applicability.**

The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.

**§ 164.402 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or per-

son acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would