

component that performs covered functions if the two components were separate legal entities.

(b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of subparts C and E of this part.

(1) *Implementation specifications:*

(i) *Requirements for designation of an affiliated covered entity.*

(A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of subparts C and E of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that:

(A) The affiliated covered entity's creation, receipt, maintenance, or transmission of electronic protected health information complies with the applicable requirements of subpart C of this part;

(B) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of subpart E of this part; and

(C) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with § 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.

5. A new subpart C is added to part 164 to read as follows:

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

Sec.

164.302 Applicability.

164.304 Definitions.

164.306 Security standards: General rules.

164.308 Administrative safeguards.

164.310 Physical safeguards.

164.312 Technical safeguards.

164.314 Organizational requirements.

164.316 Policies and procedures and documentation requirements.

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

#### **Appendix A to Subpart C of Part 164—Security Standards: Matrix**

**Authority:** 42 U.S.C. 1320d–2 and 1320d–4.

#### **§ 164.302 Applicability.**

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

#### **§ 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 subpart 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 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 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, 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.

#### **§ 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.