AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Subpart A—General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104–191, and sections 13400–13424 of Public Law 111–5.

[78 FR 5692, Jan. 25, 2013]

§ 164.103 Definitions.

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

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with §164.105(a)(2)(iii)(D).

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph §164.105(a)(2)(iii)(D).

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

[68 FR 8374, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 34266, June 7, 2013]

§ 164.104 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.

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

§ 164.105 Organizational requirements.

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this part, other than the requirements of this section, §§164.314, and 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) *Implementation specifications:*

aworley on LAPBH6H6L3 with DISTILLER
VerDate Sep<11>2014 11:32 Nov 02, 2023 Jkt 259202 PO 00000 Frm 00640 Fmt 8010 Sfmt 8010 Q:\45\45V2.TXT PC31

(i) *Application of other provisions.* In applying a provision of this part, other than the requirements of this section, §§ 164.314, and 164.504, to a hybrid entity:

(A) A reference in such provision to a ''covered entity'' refers to a health care component of the covered entity;

(B) A reference in such provision to a ''health plan,'' ''covered health care provider,'' or ''health care clearinghouse,'' refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable;

(C) A reference in such provision to ''protected health information'' refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to ''electronic protected health information'' refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part.

(iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part.

(B) The covered entity is responsible for complying with §§ 164.316(a) and 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for complying with §§ 164.314 and 164.504 regarding business associate arrangements and other organizational requirements.

(D) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates one or more health care components, it must include any component that would meet the definition of a covered entity or business associate if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs covered functions.

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

(2) *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 this part, if all of the covered

aworley on LAPBH6H6L3 with DISTILLER
VerDate Sep<11>2014 11:32 Nov 02, 2023 Jkt 259202 PO 00000 Frm 00641 Fmt 8010 Sfmt 8010 Q:\45\45V2.TXT PC31

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 it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, §§ 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.

aworley on LAPBH6H6L3 with DISTILLER
VerDate Sep<11>2014 11:32 Nov 02, 2023 Jkt 259202 PO 00000 Frm 00642 Fmt 8010 Sfmt 8010 Q:\45\45V2.TXT PC31