(Pub. L. 111–5, div. A, title XIII, § 13202, Feb. 17, 2009, 123 Stat. 245; Pub. L. 114–329, title I, § 105(s), Jan. 6, 2017, 130 Stat. 2985.)

AMENDMENTS

2017—Subsec. (b). Pub. L. 114–329 substituted ''Networking and Information Technology Research and Development Program'' for ''National High-Performance Computing Program''.

SUBCHAPTER III—PRIVACY

§ 17921. Definitions

In this subchapter, except as specified otherwise:

(1) Breach

(A) In general

The term ''breach'' means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

(B) Exceptions

The term ''breach'' does not include—

(i) any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if—

(I) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and

(II) such information is not further acquired, accessed, used, or disclosed by any person; or

(ii) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at[1] same facility; and

(iii) any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

(2) Business associate

The term ''business associate'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(3) Covered entity

The term ''covered entity'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(4) Disclose

The terms ''disclose'' and ''disclosure'' have the meaning given the term ''disclosure'' in section 160.103 of title 45, Code of Federal Regulations.

(5) Electronic health record

The term ''electronic health record'' means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

(6) Health care operations

The term ''health care operation'' has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations.

(7) Health care provider

The term ''health care provider'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(8) Health plan

The term ''health plan'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(9) National Coordinator

The term ''National Coordinator'' means the head of the Office of the National Coordinator for Health Information Technology established under section 300jj–11(a) of this title, as added by section 13101.[2]

(10) Payment

The term ''payment'' has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations.

(11) Personal health record

The term ''personal health record'' means an electronic record of PHR identifiable health information (as defined in section 17937(f)(2) of this title) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

(12) Protected health information

The term ''protected health information'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(13) Secretary

The term ''Secretary'' means the Secretary of Health and Human Services.

(14) Security

The term ''security'' has the meaning given such term in section 164.304 of title 45, Code of Federal Regulations.

(15) State

The term ''State'' means each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

(16) Treatment

The term ''treatment'' has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations.

(17) Use

The term ''use'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(18) Vendor of personal health records

The term ''vendor of personal health records'' means an entity, other than a cov-

[1] So in original. Probably should be followed by ''the''.

[2] See References in Text note below.

ered entity (as defined in paragraph (3)), that offers or maintains a personal health record.

(Pub. L. 111–5, div. A, title XIII, § 13400, Feb. 17, 2009, 123 Stat. 258.)

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original ''this subtitle'', meaning subtitle D (§ 13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

Section 13101, referred to in par. (9), means section 13101 of div. A of Pub. L. 111–5.

PART A—IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS

§ 17931. Application of security provisions and penalties to business associates of covered entities; annual guidance on security provisions

(a) Application of security provisions

Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title[1] that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

(b) Application of civil and criminal penalties

In the case of a business associate that violates any security provision specified in subsection (a), sections 1320d–5 and 1320d–6 of this title shall apply to the business associate with respect to such violation in the same manner such sections apply to a covered entity that violates such security provision.

(c) Annual guidance

For the first year beginning after February 17, 2009, and annually thereafter, the Secretary of Health and Human Services shall, after consultation with stakeholders, annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the sections referred to in subsection (a) and the security standards in subpart C of part 164 of title 45, Code of Federal Regulations, including the use of standards developed under section 300jj–12(b)(2)(B)(vi)[1] of this title, as added by section 13101 of this Act, as such provisions are in effect as of the date before February 17, 2009.

(Pub. L. 111–5, div. A, title XIII, § 13401, Feb. 17, 2009, 123 Stat. 260.)

REFERENCES IN TEXT

This title, referred to in subsec. (a), is title XIII of div. A of Pub. L. 111–5, which enacted this chapter and subchapter XXVIII (§ 300jj et seq.) of chapter 6A this title, amended sections 1320d, 1320d–5, and 1320d–6 of this title, and enacted provisions set out as a note under this section and section 201 of this title. For complete classification of title XIII to the Code, see Short Title of 2009 Amendment note set out under section 201 of this title and Tables.

[1] See References in Text note below.

Section 300jj–12(b)(2)(B)(vi) of this title, referred to in subsec. (c), was repealed by Pub. L. 114–255, div. A, title IV, § 4003(e)(1), Dec. 13, 2016, 130 Stat. 1168. Similar provisions as pertaining to the HIT Advisory Committee are contained in section 300jj–12(b)(2)(C)(vii) of this title as enacted by Pub. L. 114–255.

Section 13101 of this Act, referred to in subsec. (c), means section 13101 of div. A of Pub. L. 111–5.

EFFECTIVE DATE

Pub. L. 111–5, div. A, title XIII, § 13423, Feb. 17, 2009, 123 Stat. 276, provided that: ''Except as otherwise specifically provided, the provisions of part I [probably means part 1 (§§ 13401–13411) of subtitle D of title XIII of div. A of Pub. L. 111–5, enacting this part and amending sections 1320d–5 and 1320d–6 of this title] shall take effect on the date that is 12 months after the date of the enactment of this title [Feb. 17, 2009].''

§ 17932. Notification in the case of breach

(a) In general

A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.

(b) Notification of covered entity by business associate

A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.

(c) Breaches treated as discovered

For purposes of this section, a breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.

(d) Timeliness of notification

(1) In general

Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b)).

(2) Burden of proof

The covered entity involved (or business associate involved in the case of a notification