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 covered 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.)

Editorial Notes

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.)

Editorial Notes

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.

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.

Statutory Notes and Related Subsidiaries

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 unse-

[1] See References in Text note below.

cured 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 required under subsection (b)), shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.

(e) Methods of notice

(1) Individual notice

Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form:

(A) Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

(B) In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual under subparagraph (A), electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the Secretary on the home page of the Web site of the covered entity involved or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

(C) In any case deemed by the covered entity involved to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity, in addition to notice provided under subparagraph (A), may provide information to individuals by telephone or other means, as appropriate.

(2) Media notice

Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach described in subsection (a), if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

(3) Notice to Secretary

Notice shall be provided to the Secretary by covered entities of unsecured protected health information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals than[1] such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the covered entity may maintain a log of any such breach occurring and annually submit such a log to the Secretary documenting such breaches occurring during the year involved.

(4) Posting on HHS public website

The Secretary shall make available to the public on the Internet website of the Department of Health and Human Services a list that identifies each covered entity involved in a breach described in subsection (a) in which the unsecured protected health information of more than 500 individuals is acquired or disclosed.

(f) Content of notification

Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

(2) A description of the types of unsecured protected health information that were in-

[1] So in orginal. Probably should be ''then''.

volved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).

(3) The steps individuals should take to protect themselves from potential harm resulting from the breach.

(4) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(g) Delay of notification authorized for law enforcement purposes

If a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed in the same manner as provided under section 164.528(a)(2) of title 45, Code of Federal Regulations, in the case of a disclosure covered under such section.

(h) Unsecured protected health information

(1) Definition

(A) In general

Subject to subparagraph (B), for purposes of this section, the term ''unsecured protected health information'' means protected health information that is not secured through the use of a technology or methodology specified by the Secretary in the guidance issued under paragraph (2).

(B) Exception in case timely guidance not issued

In the case that the Secretary does not issue guidance under paragraph (2) by the date specified in such paragraph, for purposes of this section, the term ''unsecured protected health information'' shall mean protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

(2) Guidance

For purposes of paragraph (1) and section 17937(f)(3) of this title, not later than the date that is 60 days after February 17, 2009, the Secretary shall, after consultation with stakeholders, issue (and annually update) guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, including the use of standards developed under section 300jj–12(b)(2)(B)(vi)[2] of this title, as added by section 13101 of this Act.

[2] See References in Text note below.

(i) Report to Congress on breaches

(1) In general

Not later than 12 months after February 17, 2009, and annually thereafter, the Secretary shall prepare and submit to the Committee on Finance and the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Ways and Means and the Committee on Energy and Commerce of the House of Representatives a report containing the information described in paragraph (2) regarding breaches for which notice was provided to the Secretary under subsection (e)(3).

(2) Information

The information described in this paragraph regarding breaches specified in paragraph (1) shall include—

(A) the number and nature of such breaches; and

(B) actions taken in response to such breaches.

(j) Regulations; effective date

To carry out this section, the Secretary of Health and Human Services shall promulgate interim final regulations by not later than the date that is 180 days after February 17, 2009. The provisions of this section shall apply to breaches that are discovered on or after the date that is 30 days after the date of publication of such interim final regulations.

(Pub. L. 111–5, div. A, title XIII, § 13402, Feb. 17, 2009, 123 Stat. 260.)

Editorial Notes

REFERENCES IN TEXT

Section 300jj–12(b)(2)(B)(vi) of this title, referred to in subsec. (h)(2), 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. (h)(2), means section 13101 of div. A of Pub. L. 111–5.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

§ 17933. Education on health information privacy

(a) Regional office privacy advisors

Not later than 6 months after February 17, 2009, the Secretary shall designate an individual in each regional office of the Department of Health and Human Services to offer guidance and education to covered entities, business associates, and individuals on their rights and responsibilities related to Federal privacy and security requirements for protected health information.

(b) Education initiative on uses of health information

Not later than 12 months after February 17, 2009, the Office for Civil Rights within the Department of Health and Human Services shall