

(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.

(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.)

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.

§ 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 develop and maintain a multi-faceted national education initiative to enhance public transparency regarding the uses of protected health information, including programs to educate individuals about the potential uses of their protected health information, the effects of such uses, and the rights of individuals with respect to such uses. Such programs shall be conducted in a variety of languages and present information in a clear and understandable manner.

(Pub. L. 111-5, div. A, title XIII, §13403, Feb. 17, 2009, 123 Stat. 263.)

§ 17934. Application of privacy provisions and penalties to business associates of covered entities**(a) Application of contract requirements**

In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations, with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement of section 164.504(e) of such title. The additional requirements of this subchapter that relate to privacy 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 knowledge elements associated with contracts

Section 164.504(e)(1)(ii) of title 45, Code of Federal Regulations, shall apply to a business asso-

² See References in Text note below.

ciate described in subsection (a), with respect to compliance with such subsection, in the same manner that such section applies to a covered entity, with respect to compliance with the standards in sections 164.502(e) and 164.504(e) of such title, except that in applying such section 164.504(e)(1)(ii) each reference to the business associate, with respect to a contract, shall be treated as a reference to the covered entity involved in such contract.

(c) Application of civil and criminal penalties

In the case of a business associate that violates any provision of subsection (a) or (b), the provisions of sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d-5, 1320d-6) shall apply to the business associate with respect to such violation in the same manner as such provisions apply to a person who violates a provision of part C of title XI of such Act [42 U.S.C. 1320d et seq.].

(Pub. L. 111-5, div. A, title XIII, §13404, Feb. 17, 2009, 123 Stat. 264.)

REFERENCES IN TEXT

This subchapter, referred to in subsec. (a), 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.

The Social Security Act, referred to in subsec. (c), is act Aug. 14, 1935, ch. 531, 49 Stat. 620. Part C of title XI of the Act is classified generally to part C (§1320d et seq.) of subchapter XI of chapter 7 of this title. For complete classification of this Act to the Code, see section 1305 of this title and Tables.

§ 17935. Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format

(a) Requested restrictions on certain disclosures of health information

In the case that an individual requests under paragraph (a)(1)(i)(A) of section 164.522 of title 45, Code of Federal Regulations, that a covered entity restrict the disclosure of the protected health information of the individual, notwithstanding paragraph (a)(1)(ii) of such section, the covered entity must comply with the requested restriction if—

(1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and

(2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

(b) Disclosures required to be limited to the limited data set or the minimum necessary

(1) In general

(A) In general

Subject to subparagraph (B), a covered entity shall be treated as being in compliance with section 164.502(b)(1) of title 45, Code of Federal Regulations, with respect to the use,

disclosure, or request of protected health information described in such section, only if the covered entity limits such protected health information, to the extent practicable, to the limited data set (as defined in section 164.514(e)(2) of such title) or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively.

(B) Guidance

Not later than 18 months after February 17, 2009, the Secretary shall issue guidance on what constitutes “minimum necessary” for purposes of subpart E of part 164 of title 45, Code of Federal Regulation.¹ In issuing such guidance the Secretary shall take into consideration the guidance under section 17953(c) of this title and the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.

(C) Sunset

Subparagraph (A) shall not apply on and after the effective date on which the Secretary issues the guidance under subparagraph (B).

(2) Determination of minimum necessary

For purposes of paragraph (1), in the case of the disclosure of protected health information, the covered entity or business associate disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.

(3) Application of exceptions

The exceptions described in section 164.502(b)(2) of title 45, Code of Federal Regulations, shall apply to the requirement under paragraph (1) as of the effective date described in section 13423² in the same manner that such exceptions apply to section 164.502(b)(1) of such title before such date.

(4) Rule of construction

Nothing in this subsection shall be construed as affecting the use, disclosure, or request of protected health information that has been de-identified.

(c) Accounting of certain protected health information disclosures required if covered entity uses electronic health record

(1) In general

In applying section 164.528 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information—

(A) the exception under paragraph (a)(1)(i) of such section shall not apply to disclosures through an electronic health record made by such entity of such information; and

(B) an individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such covered entity during only the three years prior to the date on which the accounting is requested.

¹ So in original. Probably should be “Regulations.”

² See References in Text note below.