

(1) Breach of security

The term “breach of security” means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual.

(2) PHR identifiable health information

The term “PHR identifiable health information” means individually identifiable health information, as defined in section 1320d(6) of this title, and includes, with respect to an individual, information—

(A) that is provided by or on behalf of the individual; and

(B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

(3) Unsecured PHR identifiable health information**(A) In general**

Subject to subparagraph (B), the term “unsecured PHR identifiable health information” means PHR identifiable health information that is not protected through the use of a technology or methodology specified by the Secretary in the guidance issued under section 17932(h)(2) of this title.

(B) Exception in case timely guidance not issued

In the case that the Secretary does not issue guidance under section 17932(h)(2) of this title by the date specified in such section, for purposes of this section, the term “unsecured PHR identifiable health information” shall mean PHR identifiable health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and that is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

(g) Regulations; effective date; sunset**(1) Regulations; effective date**

To carry out this section, the Federal Trade Commission 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 of security that are discovered on or after the date that is 30 days after the date of publication of such interim final regulations.

(2) Sunset

If Congress enacts new legislation establishing requirements for notification in the case of a breach of security, that apply to entities that are not covered entities or business associates, the provisions of this section shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.

(Pub. L. 111-5, div. A, title XIII, §13407, Feb. 17, 2009, 123 Stat. 269.)

§ 17938. Business associate contracts required for certain entities

Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity (or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, or each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record, is required to enter into a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations and a written contract (or other arrangement) described in section 164.308(b) of such title, with such entity and shall be treated as a business associate of the covered entity for purposes of the provisions of this subchapter and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of February 17, 2009.

(Pub. L. 111-5, div. A, title XIII, §13408, Feb. 17, 2009, 123 Stat. 271.)

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.

§ 17939. Improved enforcement**(a) In general****(1) Omitted****(2) Enforcement under Social Security Act**

Any violation by a covered entity under thus¹ subchapter is subject to enforcement and penalties under section² 1176 and 1177 of the Social Security Act [42 U.S.C. 1320d-5, 1320d-6].

(b) Effective date; regulations

(1) The amendments made by subsection (a) shall apply to penalties imposed on or after the date that is 24 months after February 17, 2009.

(2) Not later than 18 months after February 17, 2009, the Secretary of Health and Human Services shall promulgate regulations to implement such amendments.

(c) Distribution of certain civil monetary penalties collected**(1) In general**

Subject to the regulation promulgated pursuant to paragraph (3), any civil monetary penalty or monetary settlement collected with respect to an offense punishable under this subchapter or section 1176 of the Social Security Act (42 U.S.C. 1320d-5) insofar as such section relates to privacy or security shall be transferred to the Office for Civil Rights of the Department of Health and Human Services to

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

² So in original. Probably should be “sections”.