given such term by the Secretary by regulation.

(4) Direct or indirect payment

For purposes of paragraph (2), the term ''direct or indirect payment'' shall not include any payment for treatment (as defined in section 164.501 of title 45, Code of Federal Regulations) of an individual.

(b) Opportunity to opt out of fundraising

The Secretary shall by rule provide that any written fundraising communication that is a healthcare operation as defined under section 164.501 of title 45, Code of Federal Regulations, shall, in a clear and conspicuous manner, provide an opportunity for the recipient of the communications to elect not to receive any further such communication. When an individual elects not to receive any further such communication, such election shall be treated as a revocation of authorization under section 164.508 of title 45, Code of Federal Regulations.

(c) Effective date

This section shall apply to written communications occurring on or after the effective date specified under section 13423.[1]

(Pub. L. 111–5, div. A, title XIII, § 13406, Feb. 17, 2009, 123 Stat. 268.)

REFERENCES IN TEXT

Section 13423, referred to in subsec. (c), means section 13423 of div. A of Pub. L. 111–5, which is set out as an Effective Date note under section 17931 of this title.

§ 17937. Temporary breach notification requirement for vendors of personal health records and other non-HIPAA covered entities

(a) In general

In accordance with subsection (c), each vendor of personal health records, following the discovery of a breach of security of unsecured PHR identifiable health information that is in a personal health record maintained or offered by such vendor, and each entity described in clause (ii), (iii), or (iv) of section 17953(b)(1)(A) of this title, following the discovery of a breach of security of such information that is obtained through a product or service provided by such entity, shall—

(1) notify each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such a breach of security; and

(2) notify the Federal Trade Commission.

(b) Notification by third party service providers

A third party service provider that provides services to a vendor of personal health records or to an entity described in clause (ii), (iii).[1] or (iv) of section 17953(b)(1)(A) of this title in connection with the offering or maintenance of a personal health record or a related product or service and that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information in such a record as a result of such services shall, following the discovery of a breach of security of such information, notify such vendor or entity, respectively, of such breach. Such notice shall include the identification of each individual whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

(c) Application of requirements for timeliness, method, and content of notifications

Subsections (c), (d), (e), and (f) of section 17932 of this title shall apply to a notification required under subsection (a) and a vendor of personal health records, an entity described in subsection (a) and a third party service provider described in subsection (b), with respect to a breach of security under subsection (a) of unsecured PHR identifiable health information in such records maintained or offered by such vendor, in a manner specified by the Federal Trade Commission.

(d) Notification of the Secretary

Upon receipt of a notification of a breach of security under subsection (a)(2), the Federal Trade Commission shall notify the Secretary of such breach.

(e) Enforcement

A violation of subsection (a) or (b) shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 57a(a)(1)(B) of title 15 regarding unfair or deceptive acts or practices.

(f) Definitions

For purposes of this section:

(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

[1] See References in Text note below.

[1] So in original. The period probably should be a comma.

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 thus[1] subchapter is subject to enforcement and penalties under section[2] 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 be used for purposes of enforcing 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.

(2) GAO report

Not later than 18 months after February 17, 2009, the Comptroller General shall submit to the Secretary a report including recommendations for a methodology under which an individual who is harmed by an act that constitutes an offense referred to in paragraph (1) may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.

(3) Establishment of methodology to distribute percentage of CMPS collected to harmed individuals

Not later than 3 years after February 17, 2009, the Secretary shall establish by regulation and based on the recommendations submitted under paragraph (2), a methodology under which an individual who is harmed by an act that constitutes an offense referred to in paragraph (1) may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.

(4) Application of methodology

The methodology under paragraph (3) shall be applied with respect to civil monetary penalties or monetary settlements imposed on or after the effective date of the regulation.

[1] So in original. Probably should be ''this''.

[2] So in original. Probably should be ''sections''.