or person designated by the individual, provided that any such choice is clear, conspicuous, and specific;

(2) if the individual makes a request to a business associate for access to, or a copy of, protected health information about the individual, or if an individual makes a request to a business associate to grant such access to, or transmit such copy directly to, a person or entity designated by the individual, a business associate may provide the individual with such access or copy, which may be in an electronic form, or grant or transmit such access or copy to such person or entity designated by the individual; and

(3) notwithstanding paragraph (c)(4) of such section, any fee that the covered entity may impose for providing such individual with a copy of such information (or a summary or explanation of such information) if such copy (or summary or explanation) is in an electronic form shall not be greater than the entity's labor costs in responding to the request for the copy (or summary or explanation).

(Pub. L. 111–5, div. A, title XIII, § 13405, Feb. 17, 2009, 123 Stat. 264; Pub. L. 114–255, div. A, title IV, § 4006(b), Dec. 13, 2016, 130 Stat. 1183.)

Editorial Notes

REFERENCES IN TEXT

Section 13423, referred to in subsec. (b)(3), 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.

Section 300jj–12(b)(2)(B)(iv) of this title, as added by section 13101, referred to in subsec. (c)(2), means section 300jj–12(b)(2)(B)(iv) of this title as added by section 13101 of div. A of Pub. L. 111–5. Section 300jj–12 of this title was repealed by Pub.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)(B)(ii) of this title as enacted by Pub. L. 114–255.

AMENDMENTS

2016—Subsec. (e)(2), (3). Pub. L. 114–255 added par. (2) and redesignated former par. (2) as (3).

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.

§ 17936. Conditions on certain contacts as part of health care operations

(a) Marketing

(1) In general

A communication by a covered entity or business associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall not be considered a health care operation for purposes of subpart E of part 164 of title 45, Code of Federal Regulations, unless the communication is made as described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501 of such title.

(2) Payment for certain communications

A communication by a covered entity or business associate that is described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501 of title 45, Code of Federal Regulations, shall not be considered a health care operation for purposes of subpart E of part 164 of title 45, Code of Federal Regulations if the covered entity receives or has received direct or indirect payment in exchange for making such communication, except where—

(A)(i) such communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication; and

(ii) any payment received by such covered entity in exchange for making a communication described in clause (i) is reasonable in amount;

(B) each of the following conditions apply—

(i) the communication is made by the covered entity; and

(ii) the covered entity making such communication obtains from the recipient of the communication, in accordance with section 164.508 of title 45, Code of Federal Regulations, a valid authorization (as described in paragraph (b) of such section) with respect to such communication; or

(C) each of the following conditions apply—

(i) the communication is made by a business associate on behalf of the covered entity; and

(ii) the communication is consistent with the written contract (or other written arrangement described in section 164.502(e)(2) of such title) between such business associate and covered entity.

(3) Reasonable in amount defined

For purposes of paragraph (2), the term ''reasonable in amount'' shall have the meaning 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.)

Editorial Notes

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.

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.

§ 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 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.

[1] See References in Text note below.

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