PART 318 — HEALTH BREACH NOTIFICATION RULE

Sec.

318.1 Purpose and scope.
318.2 Definitions.
318.3 Breach notification requirement.
318.4 Timeliness of notification.
318.5 Methods of notice.
318.6 Content of notice.
318.7 Enforcement.
318.8 Effective date.
318.9 Sunset.

16 C.F.R. § 318.1 Purpose and scope.

(a) This Part, which shall be called the "Health Breach Notification Rule," implements section 13407 of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. 17937. It applies to foreign and domestic vendors of personal health records, PHR related entities, and third party service providers, irrespective of any jurisdictional tests in the Federal Trade Commission (FTC) Act, that maintain information of U.S. citizens or residents. It does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity.

(b) This Part preempts state law as set forth in section 13421 of the American Recovery and Reinvestment Act of 2009~~.~~, 42 U.S.C. 17951.

16 C.F.R. § 318.2 Definitions.

(a) *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. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information. A breach of security includes an unauthorized acquisition of unsecured PHR identifiable health information in a personal health record that occurs as a result of a data breach or an unauthorized disclosure.

(b) *Business associate* means a business associate under the Health Insurance Portability and Accountability Act, ~~,~~Public Law 104-191, 110 Stat. 1936, as defined in ~~.~~45 CFR 160.103.

(c) *Clear and conspicuous* means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(1) *Reasonably Understandable*: You make your notice reasonably understandable if you:

(i) Present the information in the notice in clear, concise sentences, paragraphs, and sections;

(ii) Use short explanatory sentences or bullet lists whenever possible;

(iii) Use definite, concrete, everyday words and active voice whenever possible;

(iv) Avoid multiple negatives;

(v) Avoid legal and highly technical business terminology whenever possible; and

(vi) Avoid explanations that are imprecise and readily subject to different interpretations.

(2) *Designed to call attention.* You design your notice to call attention to the nature and significance of the information in it if you:

(i) Use a plain-language heading to call attention to the notice;

(ii) Use a typeface and type size that are easy to read;

(iii)Provide wide margins and ample line spacing;

(iv)Use boldface or italics for key words; and

(v) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information. The notice should stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

(3) *Notices on web sites or within-application messaging.* If you provide a notice on a web page or using within-application messaging, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site or software application (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and you either:

(i) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(d) Electronic mail means (1) email in combination with one or more of the following: (2) text message, within-application messaging, or electronic banner.

(e) Health care services or supplies includes any online service such as a website, mobile application, or Internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools.

(f) Health care provider means a provider of services (as defined in 42 U.S.C. 1395x(u)), a provider of medical or other health services (as defined in 42 U.S.C. 1395x(s)), or any other entity furnishing health care services or supplies.

(g) *HIPAA*-covered entity means a covered entity under the Health Insurance Portability and Accountability Act, ~~,~~Public Law 104-191, 110 Stat. 1936, as defined in ~~.~~45 CFR 160.103.

(~~d~~h) *Personal health record* means an electronic record of PHR identifiable health information on an individual that ~~can be drawn~~has the technical capacity to draw information from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

(~~e~~i) *PHR identifiable health information* means ~~"individually identifiable health~~ information~~,"~~ ~~as defined in section 1171(6) of the Social Security Act (), and, with respect to an individual, information: ~~:

(1) That is provided by or on behalf of the individual; ~~and~~

(2) ~~-~~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) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

(4) Is created or received by a:
(i) health care provider;
(iii) health plan (as defined in 42 U.S.C. 1320d(5));
(iv) employer; or
(v) health care clearinghouse (as defined in 42 U.S.C. 1320d(2)).

(j) *PHR related entity* means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that:

(1) Offers products or services through the ~~Web site~~website, including any online service, of a vendor of personal health records;

(2) Offers products or services through the ~~Web sites~~websites, including any online service, of HIPAA-covered entities that offer individuals personal health records; or

(3) Accesses unsecured PHR identifiable health information in a personal health record or sends unsecured PHR identifiable health information to a personal health record.

(~~g~~k) *State* means any of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

(~~h~~l) *Third party service provider* means an entity that:

(1) Provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and

(2) Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.

(~~i~~m) *Unsecured* means PHR identifiable information that is not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of the American Reinvestment and Recovery Act of 2009~~.~~, 42 U.S.C. 17932(h)(2).

(~~j~~n) *Vendor of personal health records* means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record.

16 C.F.R. § 318.3 Breach notification requirement.

(a) *In general.* In accordance with ~~§§§~~ 318.4~~,~~ (Timeliness of notification), § 318.5~~,~~ (Notice to FTC), and § 318.6~~,~~ (Content of notice), 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 PHR related entity, 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 breach of security; and

(2) Notify the Federal Trade Commission.; and

(3) Notify prominent media outlets serving a State or jurisdiction, following the discovery of a breach of security, if the unsecured PHR identifiable health information of 500 or more residents of such State or jurisdiction is, or is reasonably believed to have been, acquired during such breach.

(b) *Third party service providers.*. A third party service provider shall, following the discovery of a breach of security, provide notice of the breach to an official designated in a written contract by the vendor of personal health records or the PHR related entity to receive such notices or, if such a designation is not made, to a senior official at the vendor of personal health records or PHR related entity to which it provides services, and obtain acknowledgment from such official that such notice was received. Such notification shall include the identification of each customer of the vendor of personal health records or PHR related entity whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, acquired during such breach. For purposes of ensuring implementation of this requirement, vendors of personal health records and PHR related entities shall notify third party service providers of their status as vendors of personal health records or PHR related entities subject to this Part. While some third party service providers may access unsecured PHR identifiable health information in the course of providing services, this does not render the third party service provider a PHR related entity.

(c) *Breaches treated as discovered.*. A breach of security shall be treated as discovered as of the first day on which such breach is known or reasonably should have been known to the vendor of personal health records, PHR related entity, or third party service provider, respectively. Such vendor, entity, or third party service provider shall be deemed to have knowledge of a breach if such breach is known, or reasonably should have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of such vendor of personal health records, PHR related entity, or third party service provider.

16 C.F.R. § 318.4 Timeliness of notification.

(a) In general. Except as provided in paragraph (cparagraphs (b) (Timing of notice to FTC) and (d) of this section and §318.5(c(Law enforcement exception), all notifications required under §§§ 318.3(a)(1),) (required notice to individuals), § 318.3(b) (required notice by third party service providers), and 318.5(b§ 318.3(a)(3) (required notice to media) shall be sent without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.

(b) Timing of notice to FTC. All notifications required under § 318.5(c) (Notice to FTC) involving the unsecured PHR identifiable health information of 500 or more individuals shall

be provided as soon as possible and in no case later than ten business days following the date of discovery of the breach. All logged notifications required under § 318.5(c) (Notice to FTC) involving the unsecured PHR identifiable health information of fewer than 500 individuals may be sent annually to the Federal Trade Commission no later than 60 calendar days following the end of the calendar year.

~~(b)~~(c) *Burden of proof.* The vendor of personal health records, PHR related entity, and third party service provider involved shall have the burden of demonstrating that all notifications were made as required under this Part, including evidence demonstrating the necessity of any delay.

~~(c)~~(d) *Law enforcement exception.* If a law enforcement official determines that a notification, notice, or posting required under this Part would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed. This paragraph shall be implemented in the same manner as provided under ~~,~~45 CFR 164.528(a)(2), in the case of a disclosure covered under such section.

16 C.F.R. § 318.5 Methods of notice.

(a) *Individual notice.* A vendor of personal health records or PHR related entity that discovers a breach of security shall provide notice of such breach to an individual promptly, as described in § 318.4~~,~~ (Timeliness of notification), and in the following form:

(1) Written notice~~, by first-class mail to the individual~~ at the last known address of the individual~~, or by email~~. Written notice may be sent by electronic mail, if the individual ~~is given a clear, conspicuous,~~has specified electronic mail as the primary method of communication. Any written notice sent by electronic mail must be Clear and ~~reasonable opportunity to receive notification by first-class mail, and~~Conspicuous. Where notice via electronic mail is not available or the individual has not specified electronic mail as the primary method of communication, a vendor of personal health records or PHR related entity may provide notice by first-class mail at the last known address of the individual ~~does not exercise that choice~~. If the individual is deceased, the vendor of personal health records or PHR related entity that discovered the breach must provide such notice to the next of kin of the individual if the individual had provided contact information for his or her next of kin, along with authorization to contact them. The notice may be provided in one or more mailings as information is available. Exemplar notices that vendors of personal health records or PHR related entities may use to notify individuals pursuant to this paragraph are attached as Appendix A.

(2) If, after making reasonable efforts to contact all individuals to whom notice is required under § 318.3(a), through the means provided in paragraph (a)(1) of this section, the vendor of personal health records or PHR related entity finds that contact information for ten or more individuals is insufficient or out-of-date, the vendor of personal health records or PHR related entity shall provide substitute notice, which shall be reasonably calculated to reach the individuals affected by the breach, in the following form:

(i) Through a conspicuous posting for a period of 90 days on the home page of its ~~Web site~~website; or

(ii) 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 shall include a toll-free phone number, which shall remain active for at least 90 days, where an individual can learn whether or not the ~~individual's~~individual's unsecured PHR identifiable health information may be included in the breach.

(3) In any case deemed by the vendor of personal health records or PHR related entity to require urgency because of possible imminent misuse of unsecured PHR identifiable health information, that entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (a)(1) of this section.

(b) *Notice to media*. As described in § 318.3(a)(3), a vendor of personal health records or PHR related entity shall provide notice to prominent media outlets serving a State or jurisdiction, following the discovery of a breach of security, if the unsecured PHR identifiable health information of 500 or more residents of such State or jurisdiction is, or is reasonably believed to have been, acquired during such breach.

(c) *Notice to FTC.* Vendors of personal health records and PHR related entities shall provide notice to the Federal Trade Commission following the discovery of a breach of security~~. If the breach involves the unsecured PHR identifiable health information of 500 or more individuals, then such notice shall be provided as soon as possible and in no case later than ten business days following the date of discovery of the breach.~~ , as described in § 318.4(b) (Timing of notice to FTC). If the breach involves the unsecured PHR identifiable health information of fewer than 500 individuals, the vendor of personal health records or PHR related entity may maintain a log of any such breach~~,~~ and submit such a log annually to the Federal Trade Commission ~~no later than 60 calendar days following the end~~as described in § 318.4(b) (Timing of ~~the calendar year,~~notice to FTC), documenting breaches from the preceding calendar year. All notices pursuant to this paragraph shall be provided according to instructions at the Federal Trade Commission's ~~Web site.~~ website.

16 C.F.R. § 318.6 Content of notice.

Regardless of the method by which notice is provided to individuals under § 318.5 (Methods of notice) of this Part, notice of a breach of security shall be in plain language and include, to the extent possible, the following:

(a) A brief description of what happened, including: the date of the breach and the date of the discovery of the breach, if known; the potential harm that may result from the breach, such as medical or other identity theft; and the full name, website, and contact information (such as a public email address or phone number) of any third parties that acquired unsecured PHR identifiable health information as a result of a breach of security, if this information is known to the vendor of personal health records or PHR related entity;

(b) A description of the types of unsecured PHR identifiable health information that were involved in the breach (such as but not limited to full name, Social Security number, date of birth, home address, account number, ~~or disability code);~~ health diagnosis or condition, lab results, medications, other treatment information, the individual's use of a health-related mobile application, or device identifier (in combination with another data element));

(c) Steps individuals should take to protect themselves from potential harm resulting from the breach;

(d) A brief description of what the entity that ~~suffered~~experienced the breach is doing to investigate the breach, to mitigate harm, ~~and~~ to protect against any further breaches, and to protect affected individuals, such as offering credit monitoring or other services; and

(e) Contact procedures for individuals to ask questions or learn additional information, which ~~shall~~must include ~~a~~two or more of the following: toll-free telephone number~~, an~~; email address~~, Web site,~~; website; within-application; or postal address.

16 C.F.R. § 318.7 Enforcement.

~~A~~Any violation of this Part shall be treated as ~~an unfair or deceptive act or practice in~~ a violation of a ~~regulation~~rule promulgated under ~~§~~section 18~~(a)(1)(B)~~ of the Federal Trade Commission Act ~~()~~, 15 U.S.C. 57a, regarding unfair or deceptive acts or practices, and thus subject to civil penalties (as adjusted for inflation pursuant to § 1.98 of this chapter), and the Commission will enforce this Rule in the same manner, by the same means, and with the same jurisdiction, powers, and duties as are available to it pursuant to the Federal Trade Commission Act, 15 U.S.C. 41 *et seq*.

16 C.F.R. § 318.8 Effective date.

This Part shall apply to breaches of security that are discovered on or after September 24, 2009.

16 C.F.R. § 318.9 Sunset.

If new legislation is enacted establishing requirements for notification in the case of a breach of security that apply to entities covered by this Part, the provisions of this Part shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.