AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

§ 317.3 Prohibited practices.

It shall be unlawful for any person, directly or indirectly, in connection with the purchase or sale of crude oil, gasoline, or petroleum distillates at wholesale, to:

(a) Knowingly engage in any act, practice, or course of business—including the making of any untrue statement of material fact—that operates or would operate as a fraud or deceit upon any person; or

(b) Intentionally fail to state a material fact that under the circumstances renders a statement made by such person misleading, provided that such omission distorts or is likely to distort market conditions for any such product.

§ 317.4 Preemption.

The Federal Trade Commission does not intend, through the promulgation of this Rule, to preempt the laws of any state or local government, except to the extent that any such law conflicts with this Rule. A law is not in conflict with this Rule if it affords equal or greater protection from the prohibited practices set forth in § 317.3.

§ 317.5 Severability.

The provisions of this Rule are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

PART 318—HEALTH BREACH NOTIFICATION RULE

Sec.

AUTHORITY: Public Law 111-5, 123 Stat. 115 (2009).

SOURCE: 74 FR 42980, Aug. 25, 2009, unless otherwise noted.

§ 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. 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.

§ 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.

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

(e) *PHR identifiable health information* means ''individually identifiable health information,'' as defined in section

1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), 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.

(f) *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 of a vendor of personal health records;

(2) Offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records; or

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

(g) *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) *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) *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.

(j) *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.

§ 318.3 Breach notification requirement.

(a) *In general.* In accordance with §§ 318.4, 318.5, and 318.6, 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.

(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.

(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.

§ 318.4 Timeliness of notification.

(a) *In general.* Except as provided in paragraph (c) of this section and § 318.5(c), all notifications required under §§ 318.3(a)(1), 318.3(b), and 318.5(b) shall be sent without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.

(b) *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) *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.

§ 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, 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, if the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and 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.

(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; 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 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.* 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. 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 of the calendar year, 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.

§ 318.6 Content of notice.

Regardless of the method by which notice is provided to individuals under § 318.5 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;

(b) A description of the types of unsecured PHR identifiable health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code);

(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 the breach is doing to investigate the breach, to mitigate harm, and to protect against any further breaches; and

(e) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web site, or postal address.

§ 318.7 Enforcement.

A violation of this part shall be treated as an unfair or deceptive act or practice in violation of a regulation under § 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

§ 318.8 Effective date.

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

§ 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.

PART 320—DISCLOSURE REQUIREMENTS FOR DEPOSITORY INSTITUTIONS LACKING FEDERAL DEPOSIT INSURANCE

AUTHORITY: 12 U.S.C. 1831t; 15 U.S.C. 41 *et seq.*

SOURCE: 77 FR 22203, Apr. 13, 2012, unless otherwise noted.

§ 320.1 Cross-reference.

The rules formerly at 16 CFR part 320 have been republished by the Consumer Financial Protection Bureau at 12 CFR part 1009, ''Disclosure Requirements for Depository Institutions Lacking Federal Deposit Insurance (Regulation I).''

PART 321—MORTGAGE ACTS AND PRACTICES—ADVERTISING

AUTHORITY: Pub. L. 111–8, section 626, 123 Stat. 524, as amended by Pub. L. 111–24, section 511, 123 Stat. 1734.

SOURCE: 77 FR 22203, Apr. 13, 2012, unless otherwise noted.

§ 321.1 Cross-reference.

The rules formerly at 16 CFR part 321 have been republished by the Consumer Financial Protection Bureau at 12 CFR part 1014, ''Mortgage Acts and Practices Advertising (Regulation N).''