

## Federal Trade Commission

## § 318.2

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.

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

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.

### § 318.3

### 16 CFR Ch. I (1–1–10 Edition)

(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