[Billing Code 6750-01S]

FEDERAL TRADE COMMISSION

16 CFR Part 318

[RIN 3084-AB17]

Health Breach Notification Rule

AGENCY: Federal Trade Commission (FTC).

ACTION: Notice of proposed rulemaking; request for public comment.

SUMMARY: Under the American Recovery and Reinvestment Act of 2009 (the "Recovery Act" or "the Act"), the Federal Trade Commission ("FTC") or ("Commission") must issue rules requiring vendors of personal health records and related entities to notify individuals when the security of their individually identifiable health information is breached. Accordingly, the FTC seeks comment on a proposed rule.

DATES: Comments must be received on or before June 1, 2009.

ADDRESSES: Interested parties are invited to submit written comments electronically or in paper form. Comments should refer to "Health Breach Notification Rulemaking, Project No. R911002" to facilitate the organization of comments. Please note that your comment – including your name and your state – will be placed on the public record of this proceeding, including on the publicly accessible FTC website, at http://www.ftc.gov/os/publiccomments.shtm.

Because comments will be made public, they should not include any sensitive personal information, such as an individual's Social Security number; date of birth; driver's license number, state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. Comments

also should not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, comments should not include any "[t]rade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential . . . ," as provided in Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2). Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c), 16 CFR 4.9(c). [1]

Because paper mail addressed to the FTC is subject to delay due to heightened security screening, please consider submitting your comments in electronic form. Comments filed in electronic form should be submitted by using the weblink https://secure.commentworks.com/healthbreachnotification, and following the instructions on the web-based form. To ensure that the Commission considers an electronic comment, you must file it on the web-based form at the weblink https://secure.commentworks.com/healthbreachnotification. If this Notice appears at http://www.regulations.gov/search/index.jsp, you also may file an electronic comment through that website. The Commission will consider all comments that regulations.gov forwards to it. You also may visit the FTC website at http://www.ftc.gov to read the Notice and the news release describing it.

[1] See also FTC Rule 4.2(d), 16 CFR 4.2(d). The comment must be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. See FTC Rule 4.9(c), 16 CFR 4.9(c).

A comment filed in paper form should include the "Health Breach Notification Rulemaking, Project No. R911002" reference both in the text and on the envelope, and should be mailed or delivered to the following address: Federal Trade Commission/Office of the Secretary, Room H-135 (Annex M), 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The FTC is requesting that any comment filed in paper form be sent by courier or overnight service, if possible, because U.S. postal mail in the Washington area and at the Commission is subject to delay due to heightened security precautions.

The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives, whether filed in paper or electronic form. Comments received will be available to the public on the FTC website, to the extent practicable, at http://www.ftc.gov/os/publiccomments.shtm. As a matter of discretion, the Commission makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the FTC website. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at http://www.ftc.gov/ftc/privacy.shtm.

Comments on any proposed filing, recordkeeping, or disclosure requirements that are subject to paperwork burden review under the Paperwork Reduction Act should additionally be submitted to: Office of Information and Regulatory Affairs, Office of

Management and Budget ("OMB"), Attention: Desk Officer for Federal Trade Commission. Comments should be submitted via facsimile to (202) 395-5167 because U.S. postal mail at the OMB is subject to delays due to heightened security precautions.

FOR FURTHER INFORMATION CONTACT: Cora Tung Han or Maneesha Mithal, Attorneys, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580, (202) 326-2252.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Background

On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act of 2009 (the "Recovery Act" or "the Act") into law.[2] The Act includes provisions to advance the use of health information technology and, at the same time, strengthen privacy and security protections for health information.

Among other things, the Recovery Act recognizes that there are new types of web-based entities that collect consumers' health information. These entities include

[2] American Recovery & Reinvestment Act of 2009, Pub.L. 111-5, __ Stat. __.

vendors of personal health records and online applications that interact with such personal health records. Some of these entities are not subject to the privacy and security requirements of the Health Insurance Portability and Accountability Act ("HIPAA").[3] For such entities, the Recovery Act requires the Department of Health and Human Services ("HHS") to study, in consultation with the FTC, potential privacy, security, and breach notification requirements and submit a report to Congress containing recommendations within one year of enactment of the Recovery Act. Until Congress enacts new legislation implementing any recommendations contained in the HHS/FTC report, the Recovery Act contains temporary requirements, to be enforced by the FTC, that such entities notify customers in the event of a security breach.[4] The proposed rule implements these requirements.

The Recovery Act also directs HHS to promulgate interim final regulations requiring (1) HIPAA-covered entities, such as hospitals, doctors' offices, and health insurance plans, to notify individuals in the event of a security breach and (2) business associates of HIPAA-covered entities to notify such covered entities in the event of a security breach. To the extent that FTC-regulated entities engage in activities as business associates of HIPAA-covered entities, such entities will be subject only to HHS' rule requirements and not the FTC's rule requirements, as explained below. In addition, the

[3] Health Insurance Portability & Accountability Act, Pub.L. 104-191, 110 Stat. 1936 (1996).

[4] Section 13407(g)(1) of the Recovery Act requires the FTC to promulgate, within 180 days of its enactment, regulations on the breach of security notification provisions applicable to its regulated entities.

Commission notes that many of the breach notification requirements applicable to FTC-regulated entities are the same as the breach notification requirements applicable to HHS-regulated entities. Indeed, section 13407 of the Recovery Act states that the statutory requirements for timeliness, method, and content of breach notifications contained in section 13402 (the section applicable to HHS-regulated entities) shall apply to FTC-regulated entities "in a manner specified by the Federal Trade Commission." Thus, the FTC is consulting with HHS to harmonize its proposed rule with HHS' proposed rule.

II. Section-by-Section Analysis of the Proposed Rule

The Commission proposes to issue the Health Breach Notification Rule as a new Part 318 of 16 CFR. The following is a section-by-section analysis of the proposed rule.

Proposed section 318.1: Purpose and scope.

Proposed section 318.1 serves three purposes. First, it states the relevant statutory authority for the proposed rule. Second, it identifies the entities to which the proposed rule would apply: vendors of personal health records, PHR[5] related entities, and third party service providers. Third, proposed section 318.1 clarifies that the proposed rule does not apply to HIPAA-covered entities or to an entity's activities as a business associate of a HIPAA-covered entity.

The Commission also notes that the proposed rule applies to entities beyond the FTC's traditional jurisdiction under Section 5 of the FTC Act, since the Recovery Act does not limit the FTC's enforcement authority to its enforcement jurisdiction under Section 5. Indeed, section 13407 of the Recovery Act expressly applies to "vendors of

[5] PHR means personal health record.

personal health records and other non-HIPAA covered entities," without regard to whether such entities fall within the FTC's enforcement jurisdiction. Thus, the proposed rule would apply to entities such as non-profit entities that offer personal health records or related products and services, as well as non-profit third party service providers.

With respect to the scope of the proposed rule, the Commission seeks comment on (1) the nature of entities to which its proposed rule would apply; (2) the particular products and services they offer; (3) the extent to which vendors of personal health records, PHR related entities, and third party service providers may be HIPAA-covered entities or business associates of HIPAA-covered entities; (4) whether some vendors of personal health records may have a dual role as a business associate of a HIPAA-covered entity and a direct provider of personal health records to the public; and (5) circumstances in which such a dual role might lead to consumers' receiving multiple breach notices or receiving breach notices from an unexpected entity, and whether and how the rule should address such circumstances.

Proposed section 318.2: Definitions.

This section defines terms used in the Health Breach Notification Rule.

Breach of security.

The first sentence of proposed paragraph (a) defines "breach of security" as the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual. This sentence is

identical to the definition of "breach of security" in section 13407(f)(1) of the Recovery Act.

In some cases, it will be fairly easy to determine whether unsecured PHR identifiable health information has been acquired without authorization. Examples of such cases include the theft of a laptop containing unsecured personal health records; the theft of hard copies of such records; the unauthorized downloading or transfer of such records by an employee; and the electronic break-in and remote copying of such records by a hacker.

In other cases, there may be unauthorized access to data, but it is unclear, without further investigation, whether the data also has been acquired. Unauthorized persons may have access to information if it is available to them. The term acquisition, however, suggests that the information is not only available to unauthorized persons, but in fact has been obtained by them.

For example, if an entity's access log shows that an unauthorized employee obtained access to information by opening an online database of personal health records, there clearly has been access to the data, but it is not clear whether the data also has been acquired. Consider the following possible scenarios:

(1) the employee viewed the records to find health information about a particular public figure and sold the information to a national gossip magazine;

(2) the employee viewed the records to obtain information about his or her friends;

(3) the employee inadvertently accessed the database, realized that it was not the one he or she intended to view, and logged off without reading, using, or disclosing anything.

In scenario (3), the Commission believes that no acquisition has taken place; thus, breach notification is not required. Unauthorized acquisition has, however, occurred in scenarios (1) and (2).

In the types of situations described above, where there has been unauthorized access to unsecured PHR identifiable health information, the Commission believes that the entity that experienced the breach is in the best position to determine whether unauthorized acquisition has taken place. Thus, the proposed rule creates a presumption that unauthorized persons have acquired information if they have access to it, thus creating the obligation to provide breach notification. This presumption can be rebutted with reliable evidence showing that the information was not or could not reasonably have been acquired. Such evidence can be obtained by, among other things, conducting appropriate interviews of employees, contractors, or other third parties; reviewing access logs and sign-in sheets; and/or examining forensic evidence.

For example, if an entity's employee loses a laptop containing unsecured health information in a public place, the information would be accessible to unauthorized persons, giving rise to a presumption that unauthorized acquisition has occurred. The entity can rebut this presumption by showing that the laptop was recovered, and that

forensic analysis revealed that files were never opened, altered, transferred, or otherwise compromised.

Accordingly, the Commission proposes to add a second sentence to the definition of breach of security as follows: "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, any unauthorized acquisition of such information."

Business associate.

Proposed paragraph (b) defines "business associate" to mean a business associate under HIPAA, as defined in 45 CFR 160.103. That regulation, in relevant part, defines a business associate as an entity that (1) provides certain functions or activities on behalf of a HIPAA-covered entity or (2) provides "legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for" a HIPAA-covered entity.

HIPAA-covered entity.

Proposed paragraph (c) defines "HIPAA-covered entity" to mean a covered entity under HIPAA, as defined in 45 CFR 160.103. That regulation provides that a HIPAA-covered entity is a health care provider that conducts certain transactions in electronic form, a health care clearinghouse (which provides certain data processing services for health information), or a health plan.

Personal health record.

Proposed paragraph (d) defines a "personal health record" as 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." This language is substantively identical to the definition of personal health record in section 13400(11) of the Recovery Act.[6]

PHR identifiable health information.

Proposed paragraph (e) defines "PHR identifiable health information" as "individually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)),[7] 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

[6] Where this Notice characterizes an element of the proposed rule as "substantively identical" to a corresponding provision in the Recovery Act, the difference between the two texts is minor and not substantive, and the relevant text of both the rule and statute is intended to have the same meaning. For example, the Recovery Act's definition of "personal health record" states that it is an "electronic record of PHR identifiable health information (as defined in section 13407(f)(2)). . ." The proposed rule definition drops the cross-reference, but is identical in all other respects. In other places, the rule may change a plural to a singular or vice versa; substitute terminology such as "HIPAA-covered entity" for "covered entity"; spell out a shorthand notation in the statute; or make similar non-substantive changes.

[7] This provision defines "individually identifiable health information" as information that "(1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) 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."

used to identify the individual." This definition is substantively identical to section 13407(f)(2) of the Recovery Act.

The Commission notes three points with respect to this definition. First, because the definition of "PHR identifiable health information" includes information that relates to the "past, present, or future payment for the provision of health care to an individual," the proposed rule covers breaches of such information. Thus, for example, the proposed rule would cover a security breach of a database containing names and credit card information, even if no other information was included.

Second, because the definition includes information that relates to "the health or condition" of the individual, it would include the fact of having an account with a vendor of personal health records or related entity, where the products or services offered by such vendor or related entity relate to particular health conditions. For example, the theft of an unsecured customer list of a vendor of personal health records or related entity directed to AIDS patients or people with mental illness would require a breach notification, even if no specific health information is contained in that list.

Third, if there is no reasonable basis to believe that information can be used to identify an individual, the information is not "PHR identifiable health information," and a breach notification need not be provided. For example, if a breach involves information that has been "de-identified" under HHS rules implementing HIPAA, the Commission will deem that information to fall outside the scope of "PHR identifiable health information" and therefore not covered by the proposed rule. The HHS rules

specify two ways to de-identify information: (1) if there has been a formal determination by a qualified statistician that information has been de-identified; or (2) if specific identifiers about the individual, the individual's relatives, household members, and employers are removed, and the covered entity has no actual knowledge that the remaining information could be used to identify the individual.[8] There may be additional instances where, even though the standard for de-identification under 45 CFR 164.514(b) is not met, there is no reasonable basis to believe that information is individually identifiable. The Commission requests examples of such instances.

PHR related entity.

Proposed paragraph (f) defines the term "PHR related entity" to cover the three types of entities set forth in clauses (ii), (iii), and (iv) of section 13424(b)(1)(A) of the Recovery Act.[9] First, the definition includes entities that are not HIPAA-covered entities and that offer products or services through the website of a vendor of personal health records. This definition is substantively identical to the statutory language but also clarifies that HIPAA-covered entities are excluded. This clarification is consistent with the coverage of section 13424, which requires a study and report on the "Application of Privacy and Security Requirements to Non-HIPAA Covered Entities."

---

[8] 45 CFR 164.514(b); see also U.S. Department of Health and Human Services, OCR Privacy Brief: Summary of the HIPAA Privacy Rule, www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[9] At the outset, proposed paragraph (f) clarifies that the term excludes HIPAA-covered entities, as well as other entities to the extent that they engage in activities as a business associate of a HIPAA-covered entity.

Examples of entities that could fall within this category include a web-based application that helps consumers manage medications; a website offering an online personalized health checklist; and a brick-and-mortar company advertising dietary supplements online. Consumers interact with entities in this category by clicking on the appropriate link on the website of a vendor of personal health records.

Second, PHR related entities include entities that are not HIPAA-covered entities and that offer products or services through the websites of HIPAA-covered entities that offer individuals personal health records. This language is substantively identical to section 13424(b)(1)(A)(iii) of the Recovery Act. This category differs from the first category in that it covers entities whose applications are offered through the websites of HIPAA-covered entities, as opposed to non-HIPAA covered entities. Entities may fall in both categories if they offer their applications through both HIPAA-covered websites and non-HIPAA covered websites.

Third, PHR related entities include non-HIPAA covered entities "that access information in a personal health record or send information to a personal health record." This language is substantively identical to section 13424(b)(1)(A)(iv) of the Recovery Act. This category could include online applications through which individuals, for example, connect their blood pressure cuffs, blood glucose monitors, or other devices so that the results could be tracked through their personal health records. It could also include an online medication or weight tracking program that pulls information from a personal health record.

Third party service provider.

Proposed paragraph (g) defines the term "third party service provider" as "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." Because the term third party service provider is not defined in the Recovery Act, the Commission based its proposed definition on the description of third party service providers in section 13407(b) of the Act. Third party service providers include, for example, entities that provide billing or data storage services to vendors of personal health records or PHR related entities.

Unsecured.

Proposed paragraph (h) defines the term "unsecured" as "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 Recovery and Reinvestment Act of 2009." If such guidance is not issued by the date specified in such section (i.e., by 60 days after enactment of the Act and annually thereafter), the term unsecured means "not secured by a technology standard that renders PHR identifiable 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." The proposed definition is substantively identical to the definition of "unsecured PHR identifiable health information" in the Recovery Act.

Vendor of personal health records.

Proposed paragraph (i) defines the term "vendor of personal health records" to mean "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." This proposed definition is substantively identical to the statutory definition contained in section 13400(18) of the Recovery Act, but also clarifies that a vendor of personal health records does not include entities' activities as a business associate of a HIPAA-covered entity.

Proposed section 318.3: Breach notification requirement.

Proposed paragraph 318.3(a) requires vendors of personal health records and PHR related entities, upon discovery of a breach of security, to notify U.S. citizens and residents whose information was acquired in the breach and to notify the FTC. This provision is substantively identical to section 13407(a) of the Recovery Act.

Proposed paragraph 318.3(b) requires third party service providers to both vendors of personal health records and PHR related entities to provide notification to such vendors and entities following the discovery of a breach. The purpose of this requirement is to ensure that the vendor or entity receiving the breach notification is aware of the breach, so that it can in turn provide its customers with a breach notice. To

further this purpose, proposed paragraph 318.3(b) requires that the third party service provider's notification shall include "the identification of each individual" whose information "has been, or is reasonably believed to have been acquired during such breach."

The proposed paragraph is substantively identical to section 13407(b) of the Recovery Act,[10] but adds language requiring entities to provide notice to a senior official of the vendor or PHR related entity and to obtain acknowledgment from such official that he or she has received the notice. The purpose of this requirement is to avoid the situation in which lower-level employees of two entities might have discussions about a breach that never reach senior management. It is also designed to avoid the problem of lost e-mails or voicemails.

Finally, proposed section 318.3(c) provides that a breach "shall be treated as discovered as of the first day on which such breach is known to a vendor of personal health records, PHR related entity, or third party service provider, respectively, (including any person, other than the individual committing the breach, that is an

---

[10] As noted above, although the Recovery Act does not define the term "third party service provider," the proposed rule sets forth a definition based on the language in section 13407(b) describing such entities. Thus, it is not necessary to repeat the descriptive language in this section of the proposed rule.

In addition, the proposed rule requires notification to individuals whose information was "acquired," while the Recovery Act uses the terms "accessed, acquired, or disclosed." This change is intended to harmonize the proposed rule with the other provisions of the Act making clear that the standard for FTC-regulated entities, including third party service providers, is "acquired." Indeed, the statute requires third party service providers to notify individuals upon a "breach of security," which is defined only as unauthorized acquisition.

employee, officer, or other agent of such vendor of personal health records, PHR related entity, or third party service provider, respectively) or should reasonably have been known to such vendor of personal health records, PHR related entity, or third party service provider (or person) to have occurred." This proposed paragraph is substantively identical to section 13402(c) of the Recovery Act.[11]

Regarding the "reasonably should have been known" standard, the Commission expects entities that collect and store unsecured PHR identifiable health information to maintain reasonable security measures, including breach detection measures, which should assist them in discovering breaches in a timely manner. If an entity fails to maintain such measures, and thus fails to discover a breach, such failure could constitute a violation of the proposed rule because the entity "reasonably" should have known about the breach. The Commission recognizes, however, that certain breaches may be very difficult to detect, and that an entity with strong breach detection measures may nevertheless fail to discover a breach. In such circumstances, the failure to discover the breach would not constitute a violation of the proposed rule.[12]

---

[11] Section 13407(c) of the Recovery Act states that the standard for when breaches are discovered for HIPAA-covered entities also shall apply to FTC-regulated entities "in a manner specified by the Federal Trade Commission."

[12] The Commission enforces a variety of laws requiring entities to provide reasonable and appropriate security for the data that they collect from consumers. See, e.g., Federal Trade Commission Act, 5 USC 45; Fair Credit Reporting Act, 15 USC 1681-1681x; Gramm-Leach-Bliley Act, 15 USC 6801(b), and Standards for Safeguarding Customer Information, 16 CFR Part 314 ("Safeguards Rule"), available at http://www.ftc.gov/os/2002/05/67fr36585.pdf. The Commission has also disseminated educational materials encouraging companies to provide security for consumer data and providing guidance regarding practical ways to do so.

Proposed section 318.4: Timeliness of notification.[13]

Proposed section 318.4(a) requires breach notifications to individuals and the media to be made "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach. This language is substantively identical to section 13402(d)(1) of the Recovery Act, except that the Commission has clarified that the timing requirement for notice to consumers is different from the requirement for notice to the FTC. Proposed section 318.4(b) states that vendors of personal health records, PHR related entities, and third party service providers have the burden of proving that they provided the appropriate breach notifications. Finally, proposed section 318.4(c) allows breach notification to be delayed upon appropriate request of a law enforcement official. The proposed burden of proof and law enforcement provisions are substantively identical to sections 13402(d)(2) and 13402(g) of the Recovery Act.[14]

The Commission notes that the standard for timely notification is "without unreasonable delay," with the 60-day period serving as an outer limit. Thus, in some cases, it may be an "unreasonable delay" to wait until the 60th day to provide notification. For example, if a vendor of personal health records or PHR related entity learns of a breach, gathers all necessary information, and has systems in place to provide

[13] Section 13407(c) of the Recovery Act states that the requirements for timeliness of notification applicable to HIPAA-covered entities also shall apply to FTC-regulated entities "in a manner specified by the Federal Trade Commission."

[14] Section 13402(d)(1) of the Recovery Act sets forth the standard for timeliness of notification, but notes that this standard is subject to the exception for law enforcement set forth in section 13402(g).

notification within 30 days, it would be unreasonable to wait until the 60th day to send the notice. There may also be circumstances where a vendor of personal health records or PHR related entity discovers that its third party service provider has suffered a breach (e.g., through a customer or whistleblower) before the service provider notifies the vendor or entity that the breach has occurred. In such circumstances, the vendor or entity should treat this breach as "discovered" for purposes of providing timely notification, and should not wait until receiving notice from the service provider to begin taking steps to address the breach.

Proposed section 318.5: Methods of notice.[15]

Proposed section 318.5 addresses the methods of notice to individuals, the Commission, and the media in the event of a breach of security of unsecured PHR identifiable health information. The goal of this proposed section is to ensure prompt and effective notice.

Individual notice.

Proposed paragraph (a) addresses notice to individuals. It contains four main requirements. First, proposed paragraph (a)(1) states that individuals must be given notice by first-class mail or, if the individual provides express affirmative consent, by e-mail. This language is identical to section 13402(e)(1)(A) of the Recovery Act, except that it interprets the statutory phrase "specified as a preference by the individual" to mean

[15] Section 13407(c) of the Recovery Act states that the requirements for methods of breach notification applicable to HIPAA-covered entities also shall apply to FTC-regulated entities "in a manner specified by the Federal Trade Commission."

that the individual must provide "express affirmative consent" to receive breach notices by e-mail. Entities may obtain such consent by asking individuals, when they create an account, whether they would prefer to receive important notices about privacy by first-class mail or e-mail.[16]

The Commission recognizes that the relationship between a vendor of personal health records or PHR related entity and the individual takes place online. Thus, e-mail notice may be particularly well-suited to the relationship. In addition, vendors of personal health records and PHR related entities may not want to collect mailing addresses from consumers, and consumers may not want to provide them. Under the proposed rule, these entities need not collect such mailing addresses, as long as they obtain consumers' express affirmative consent to receive notices by e-mail. The Commission recognizes that some e-mail notifications may be screened by consumers' spam filters and requests comment on how to address this issue.

Second, as provided in section 13402(e)(1)(C) of the Recovery Act, proposed paragraph (a)(2) allows a vendor of personal health records or PHR related entity to provide notice by telephone or other appropriate means, in addition to the notice provided in paragraph (a)(1), if there is possible imminent misuse of unsecured PHR identifiable health information.

Third, proposed paragraph (a)(3) states that if, after making reasonable efforts to contact an individual through his or her preferred method of communication, the vendor

[16] The Commission does not regard pre-checked boxes or disclosures that are buried in a privacy policy or terms of service agreement to be sufficient to obtain consumers' "express affirmative consent."

of personal health records or PHR related entity learns that such method is insufficient or out-of-date, the vendor or related entity shall attempt to provide the individual with a substitute form of actual notice, which may include written notice through the individual's less-preferred method, a telephone call, or other appropriate means. This provision gives effect to section 13402(e)(1)(B) of the Recovery Act, which requires a substitute form of notice in the case of insufficient or out-of-date contact information, but adds clarifying language requiring reasonable efforts to provide the preferred form of notice before substitute notice can be used. Examples of reasonable efforts include: (1) where e-mail is the consumer's preferred method, attempting to e-mail the notice and receiving a return message stating that the e-mail could not be delivered; (2) where first class mail is the consumer's preferred method, attempting to mail such notice and having it returned as undeliverable; (3) in the case of incomplete contact information, searching internal records and, if needed, undertaking additional reasonable efforts to obtain complete and accurate contact information from other sources. The proposed rule also adds language stating that methods of substitute notice may include written notice by the consumer's less preferred method or telephone.

Finally, the proposed rule states that if ten or more individuals cannot be reached, the vendor of personal health records or PHR related entity must provide substitute notice in one of two forms. First, it can provide notice through the home page of its website. Second, it can provide notice in major print or broadcast media. The language in the proposed rule is substantively identical to section 13402(e)(1)(B) of the Recovery Act, but adds certain clarifying language, as noted below.

As to the first method of substitute notice, the Recovery Act states that the posting should appear for a period determined by the Commission and be "conspicuous." The Commission believes that six months is an appropriate time period for posting of the notice and has so specified in the proposed rule. Requiring a six month posting will ensure that individuals who intermittently check their accounts obtain notice, without being unduly burdensome for businesses.

To ensure conspicuousness, if an entity intends to use a hyperlink on the home page to convey the breach notice, the hyperlink should be (1) prominent so that it is noticeable to consumers, given the size, color and graphic treatment of the hyperlink in relation to other parts of the page; and (2) worded to convey the nature and importance of the information to which it leads. For example, "click here" would not be an appropriate hyperlink; a prominent "click here for an important notice about a security breach that may affect you" would be.[17]

Regarding the requirement that the notice be posted on the home page, the Commission notes that individuals who already have accounts with vendors of personal health records may be directed to a first or "landing" page that is different from the home page to which non-account holders are directed. The Commission thus construes "home page" to include both the home page for new visitors and the landing page for existing account holders. In general, the Commission anticipates that, because PHRs generally

[17] See "Dot Com Disclosures: Information about Online Advertising," http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf.

involve an online relationship, web posting would be a particularly well-suited method of substitute notice to individuals.

The alternative form of substitute notice described in this paragraph is media notice "in major print or broadcast media, including major media in geographic areas where individuals affected by the breach likely reside, which shall be reasonably calculated to reach individuals affected by the breach." This language is substantively identical to section 13402(e)(1)(B) of the Recovery Act, but also adds a clause requiring that such notice "be reasonably calculated to reach the individuals affected." Indeed, because this notice is intended to serve as a substitute for notice to particular individuals, it should be reasonably calculated to reach those individuals.

The appropriate scope of substitute media notice will depend on several factors, including the number of individuals for whom no contact information can be obtained, the location of those individuals, and the reach of the particular media used. For example, if a vendor of personal health records experiences a breach in which a hacker obtains the health records of millions of individuals nationwide, and the vendor has no contact information for these individuals, the notice should run multiple times in national print publications and on national network and cable television. In contrast, if an online weight management application loses a customer list and can reach all but 20 individuals in a particular city, it could run a more limited number of advertisements in appropriate local media.

Further, a notice can only be "reasonably calculated to reach the individuals affected" if it is clear and conspicuous. Thus, the notices should be stated in plain

language, be prominent, and run multiple times. The Commission requests further comment on the standards that should apply to substitute media notice.

As set forth in section 13402(e)(1)(B) of the Recovery Act, the proposed rule also provides that notice under paragraph (3), whether on the home page of the website or by media notice, must include a toll-free phone number where an individual can learn whether his or her unsecured PHR identifiable health information may be included in the breach. As to this requirement, the Commission notes that entities should have reasonable procedures in place to verify that they are providing the requested information only to the individual and not to an unauthorized person. For example, entities could provide the requested information pertaining to the consumer pursuant to the "preferred method" designated in paragraph (a)(1).

Notice to media.

Proposed paragraph (b) requires media notice "to prominent media outlets serving a State or jurisdiction" if there has been a breach of security of unsecured PHR identifiable health information of 500 or more residents of the state or jurisdiction.[18] This media notice differs from the substitute media notice described in paragraph 318.5 in that it is directed "to" the media and is intended to supplement, but not substitute for, individual notice. The proposed paragraph is substantively identical to section

[18] Although section 13402(e)(2) of the Recovery Act requires notice to media for breaches involving "more than 500" residents, section 13402(e)(3) requires notice to the government for breaches with respect to "500 or more" individuals. For consistency, the proposed rule uses "500 or more" for both kinds of notice.

13402(e)(2) of the Recovery Act, but adds a requirement that the notice include the information set forth in proposed section 318.6.

This media notice should, at a minimum, include the dissemination of a press release to media outlets in the area(s) affected by the breach. For example, if a breach affects consumers from a particular state or locality, the press release could be sent to the relevant division or department (e.g., health, technology, or business) of a number of state or local print publications, network and cable new shows, and radio stations. The Commission requests further comment on the standards and criteria that should apply in determining the adequacy of media notice.

Notice to the Commission.

Proposed paragraph (c) addresses notice to the Commission. Under the proposed paragraph, vendors of personal health records and PHR related entities must provide notice to the Commission as soon as possible and in no case later than five business days if the breach involves the unsecured PHR identifiable health information of 500 or more individuals. If the breach involves the unsecured PHR identifiable health information of fewer than 500 individuals, vendors of personal health records and PHR related entities may, in lieu of immediate notice, maintain a breach log and submit such a log annually to the Commission. The proposed paragraph is substantively identical to section 13402(e)(3) of the Recovery Act, but clarifies the Act's requirements as follows.

First, the paragraph interprets the term "immediately" to mean "as soon as possible, and in no case later than five business days." The Commission believes that

this period of time satisfies the requirement for immediacy, while still being sufficient for the breached entity to learn enough about the breach to provide meaningful notice to the Commission.[19]

Second, the paragraph states that the "annual log" to be submitted to the Commission for breaches involving fewer than 500 individuals shall be due one year from the date of the entity's first breach.[20] The Commission believes that specifying a date for submitting the log will assist entities in complying with the proposed rule.

Third, the paragraph references a form that the Commission plans to develop, to be posted on the Commission's website, www.ftc.gov, and to be used by entities to provide both the immediate and the annual required notice to the Commission under the proposed rule.[21] Among other things, the form will request information similar to that required to be included in a notice to individuals under section 318.6.

---

[19] The Commission recognizes that the breached entity may not learn all relevant information about the breach within five business days, such as number of consumers affected or extent of the information breached. Nonetheless, the entity should tell the Commission all that it knows and should provide additional information as it becomes available.

[20] No annual log needs to be provided for years in which no breaches occur.

[21] The Commission also will provide notice of breaches to the Secretary of HHS, as required by section 13407(d) of the Recovery Act.

Proposed section 318.6: Content of notice.[22]

Proposed section 318.6 addresses the content of the notice to individuals. It requires that the notice include a description of how the breach occurred; a description of the types of unsecured PHR identifiable health information that were involved in the breach; the steps individuals should take to protect themselves from potential harm; a description of what the vendor of personal health records or PHR related entity involved is doing to investigate the breach, to mitigate any losses, and to protect against any further breaches; and contact procedures for individuals to ask questions or learn additional information. The language in the proposed rule is substantively identical to the language of section 13402(f) of the Recovery Act. The Commission notes two points with respect to this section.

First, to ensure that notices do not raise concerns about phishing, those sending notices should not include any requests for personal or financial information.[23]

Second, the proposed rule requires that the notice identify steps individuals should take to protect themselves from potential harm. The Commission recognizes that these steps will differ depending on the circumstances of the breach and the type of PHR identifiable health information involved. In some instances – for example, if health insurance account information is compromised – there is a possibility that data will be

[22] Section 13407(c) of the Recovery Act states that the requirements for contents of breach notification applicable to HIPAA-covered entities also shall apply to FTC-regulated entities "in a manner specified by the Federal Trade Commission."

[23] Phishing is the act of sending an electronic message under false pretenses to induce unsuspecting victims to reveal personal and financial information.

misused. In such cases, the entity could suggest steps including, but not limited to, requesting and reviewing copies of medical files for potential errors; monitoring explanation of benefit forms for potential errors; contacting insurers to notify them of possible medical identity theft; following up with providers if medical bills do not arrive on time to ensure that an identity thief has not changed the billing address; and, in appropriate cases, trying to change health insurance account numbers.

If the breach also involves Social Security numbers, the entity should suggest additional steps such as placing a fraud alert on credit reports; obtaining and reviewing copies of credit reports for signs of identity theft; calling the local police or sheriff's office in the event suspicious activity is detected; and if appropriate, obtaining a credit freeze.[24] In the case of a breach involving financial account numbers, the entity also should direct consumers to monitor their accounts for suspicious activity and contact their financial institution about closing any compromised accounts. In appropriate cases, the entity also could refer consumers to the FTC's identity theft website, www.ftc.gov/idtheft.

In other instances, the likely harm will be personal embarrassment. In such cases, any steps that an individual may choose to take will likely be personal to that individual, and the entity may not be in a position to advise the consumer.

[24] In general, once a consumer initiates a credit freeze with a consumer reporting agency, the freeze prevents the agency from releasing a credit report about that consumer unless the consumer removes the freeze.

Proposed sections 318.7, 318.8, and 318.9.

Proposed sections 318.7, 318.8, and 318.9 are substantively identical to the statutory provisions on enforcement, effective date, and sunset. Proposed section 318.9 clarifies that the sunsetting of the rule is triggered when Congress enacts new legislation affecting entities subject to the FTC rule.

III. Communications by Outside Parties to Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding from any outside party to any Commissioner or Commissioner's advisor will be placed on the public record. See 16 C.F.R. 1.26(b)(5).

IV. Paperwork Reduction Act

The Commission is submitting this proposed rule and a Supporting Statement to the Office of Management and Budget for review under the Paperwork Reduction Act ("PRA") (44 USC 3501-3521). The breach notification requirements discussed above constitute "collections of information" for purposes of the PRA. See 5 CFR 1320.3(c). Accordingly, staff has estimated the paperwork burden for these requirements as set forth below.

In the event of a data breach, the proposed rule would require covered firms to investigate and, if certain conditions are met, notify consumers and the Commission. The paperwork burden of these requirements will depend on a variety of factors, including the number of covered firms; the percentage of such firms that will experience

a breach requiring further investigation and, if necessary, the sending of breach notices; and the number of consumers notified.

Based on input from industry sources, staff estimates that approximately 200 vendors of personal health records and 500 PHR related entities will be covered by the Commission's proposed rule. Thus, a total of 700 entities may be required to notify consumers and the Commission in the event that they experience a breach. Approximately 200 third party service providers also will be subject to the rule, and thus required to notify vendors of personal health records or PHR related entities in the event of a breach. Thus, a total of approximately 900 entities will be subject to the proposed rule's breach notification requirements.

Staff estimates that these entities, cumulatively, will experience 11 breaches per year for which notification may be required. Because there is insufficient data at this time about the number and incidence of breaches in the PHR industry, staff used available data relating to breaches incurred by private sector businesses in order to calculate a breach incidence rate. Staff then applied this rate to the estimated total number of entities that will be subject to the proposed rule. According to one recent research paper, private sector businesses across multiple industries experienced a total of approximately 50 breaches per year during the years 2002 through 2007.[25] Dividing 50

[25] Sasha Romanosky, Rahul Telang & Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?" Seventh Workshop on the Economics of Information Security, June 2008. The authors tallied the breaches reported to the website Attrition.org during the time period 2002 to 2007 and counted a total of 773 breaches for a range of entities, including businesses, governments, health providers, and educational institutions. Staff used the volume of breaches reported for businesses (246 over a 5 year period, or approximately 50 per year) because that class of data is most compatible with

breaches by the estimated number of firms that would be subject to a breach (4,187)[26] yields an estimated breach incidence rate of 1.2% per year. Applying this incidence rate to the estimated 900 vendors of personal health records, PHR related entities, and third party service providers yields an estimate of 11 breaches per year that may require notification of consumers and the Commission.

To determine the annual paperwork burden, staff has developed estimates for three categories of potential costs: (1) the costs of determining what information has been breached, identifying the affected customers, preparing the breach notice, and making the required report to the Commission; (2) the cost of notifying consumers; and (3) the cost of setting up a toll-free number, if needed.

First, in order to determine what information has been breached, identify the affected customers, prepare the breach notice, and make the required report to the Commission, staff estimates that covered firms will require per breach, on average, 100 hours of employee labor at a cost of $4,652,[27] and the services of a forensic expert at an

---

other data staff used to calculate the incidence of breaches.

[26] Staff focused on firms that routinely collect information on a sizeable number of consumers, thereby rendering them attractive targets for data thieves. To do so, staff focused first on retail businesses and eliminated retailers with annual revenue under $1,000,000. The 2002 Economic Census reports that, in that year, there were 418,713 retailers with revenue of $1,000,000 or more. To apply 50 breaches to such a large population, however, would yield a very small incidence rate. In an abundance of caution, to estimate more conservatively the incidence of breach, staff then assumed that only one percent of these firms had security vulnerabilities that would render them breach targets, thus yielding the total of 4,187.

[27] Hourly wages throughout this notice are based on http://www.bls.gov/ncs/ncswage2007.htm (National Compensation Survey: Occupational Earnings in the United States 2007, U.S. Department of Labor released August 2008,

estimated cost of $2,930.[28] Thus, the cost estimate for each breach will be $7,582. This estimate does not include the cost of equipment or other tangible assets of the breached firms, because they likely will use the equipment and other assets they have for ordinary business purposes. Based on the estimate that there will be 11 breaches per year, the annual cost burden for affected entities to perform these tasks will be $83,402 (11 breaches x $7,582 each).

Second, the cost of breach notifications will depend on the number of consumers contacted. Based on a recent survey, 11.6 percent of adults reported receiving a breach notification during a one-year period.[29] Staff estimates that for the prospective 3-year PRA clearance, the average customer base of all vendors of personal health records and PHR related entities will be approximately two million per year. Accordingly, staff estimates that an average of 232,000 consumers per year will receive a breach notification.

Bulletin 2704, Table 3 ("Full-time civilian workers," mean and median hourly wages).

The breakdown of labor hours and costs is as follows: 50 hours of computer and information systems managerial time at $52.56 per hour; 12 hours of marketing managerial time at $53.00 per hour; 33 hours of computer programmer time at $33.77 per hour; and 5 hours of legal staff time at 54.69 per hour.

[28] Staff estimates that breached entities will use 30 hours of a forensic expert's time. Staff applied the wages of a network systems and data communications analyst ($32.56), tripled it to reflect profits and overhead for an outside consultant ($97.68), and multiplied it by 30 hours to yield $2,930.

[29] Ponemon Institute, "National Survey on Data Security Breach Notification," 2005. Staff believes that this estimate is likely high given the importance of data security to the PHR industry and the likelihood that data encryption will be a strong selling point to consumers.

Given the online relationship between consumers and vendors of personal health records and PHR related entities, most notifications will be made by email and the cost of such notifications will be de minimis.[30]

In some cases, however, vendors of personal health records and PHR related entities will need to notify individuals by postal mail, either because these individuals have asked for such notification, or because the email addresses of these individuals are not current or not working. Staff estimates that the cost of notifying an individual by postal mail is approximately $2.30 per letter.[31] Assuming that vendors of personal health records and PHR related entities will need to notify by postal mail 10 percent of their customers whose information is breached, the estimated cost of this notification will be $53,360 per year.

In addition, vendors of personal health records and PHR related entities sometimes may need to notify consumers by posting a message on their home page, or by providing media notice. Based on a recent study on data breach costs, staff estimates the cost of providing notice via website posting to be 6 cents per breached record, and the cost of providing notice via published media to be 3 cents per breached record.[32] Applied to the

---

[30] See National Do Not Email Registry, A Report to Congress, June 2004 n.93, available at www.ftc.gov/reports/dneregistry/report.pdf.

[31] Robin Sidel and Mitchell Pacelle, "Credit-Card Breach Tests Banking Industry's Defenses," Wall Street Journal, June 21, 2005, p.C1. Sidel and Pacelle reported that industry sources estimated the cost per letter to be about $2.00 in 2005. Allowing for inflation, staff estimates the cost to average about $2.30 per letter over the next three years of prospective PRA clearance sought from OMB.

[32] Ponemon Institute, 2006 Annual Study: Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions, Table 2.

above-stated estimate of 232,000 consumers per year receiving breach notification, the estimated total annual cost of website notice will be $13,920, and the estimated total annual cost of media notice will be $6,960, yielding an estimated total annual cost for all forms of notice to consumers of $74,240.

Finally, the cost of a toll-free number will depend on the cost associated with T1 lines sufficient to handle the projected call volume, the cost of obtaining a toll-free telephone number and queue messaging (a service that provides rudimentary call routing), the cost of processing each call, and the telecommunication charges associated with each call. Because the proposed rule may require entities to notify consumers by posting a message on their homepage for a period of six months, staff estimated the cost of a toll-free line for a six-month period. Based on industry research, staff projects that in order to accommodate a sufficient number of incoming calls for that period, affected entities may need two T1 lines at a cost of $18,000.[33] Staff further estimates that the cost of obtaining a dedicated toll-free line and queue messaging will be $3,017,[34] and that processing an estimated 5,000 calls for the first month per breach will require an average of 1,917 hours of employee labor at a cost of $27,468.[35] Staff estimates that affected entities will need to

[33] According to industry research, the cost of a single T1 line is $1,500 per month.

[34] Staff estimates that installation of a toll-free number and queue messaging will require 40 hours of a technician's time. Staff applied the wages of a telecommunications technician ($25.14), tripled it to reflect profits and overhead of a telecommunications firm ($75.42), and multiplied it by 40 hours to yield $3,017.

[35] The breakdown of labor hours and costs is as follows: 667 hours of telephone operator time (8 minutes per call x 5,000 calls) at $14.87 per hour and 1,250 hours of information processor time (15 minutes per call x 5,000 calls) at $14.04 per hour.

offer the toll-free number for an additional five months, during which time staff projects that entities will receive an additional 5,000 calls per breach,[36] yielding an estimated total processing cost of $54,936. In addition, according to industry research, the telecommunication charges associated with the toll-free line will be approximately $2,500.[37] Adding these costs together, staff estimates that the cost per breach for the toll-free line will be $78,453. Based on the above rate of 11 breaches per year, the annual cost burden for affected entities will be $862,983 (11 x $78,453).

In sum, the estimated annual cost burden associated with the breach notification requirements is $1,020,625: $83,402 (costs associated with investigating breaches, drafting notifications of breaches, and notifying the Commission) + $74,240 (costs associated with notifying consumers) + $862,983 (costs associated with establishing toll-free numbers). Staff notes that this estimate likely overstates the costs imposed by the proposed rule because: (1) it assumes that all breaches will require notification, whereas many breaches (e.g., those involving data that is "not unsecured") will not require notification; (2) it assumes that all covered entities will be required to take all of the steps required above; and (3) staff made conservative assumptions in developing many of the underlying estimates.

[36] Staff anticipates that the greatest influx of calls will be in the first month, and that it will be equivalent to the volume of calls over the remaining five months.

[37] Staff estimates a cost per call of 25¢ (5¢ per minute/per call x 5 minutes per call). Assuming 10,000 calls for each breach, the total estimated telecommunications charges are $2,500.

The Commission invites comments on: (1) whether the proposed collection of information is necessary for the proper performance of the functions of the FTC, including whether the information will have practical utility; (2) the accuracy of the FTC's estimate of the burden of the proposed collection of information; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of collecting information on those who respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

V. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA), 5 U.S.C. 604(a), requires an agency either to provide an Initial Regulatory Flexibility Analysis with a proposed rule, or certify that the proposed rule will not have a significant economic impact on a substantial number of small entities. The FTC does not expect that this rule, if adopted, would have a significant economic impact on a substantial number of small entities. First, most of the burdens flow from the mandates of the Act, not from the specific provisions of the proposed rule. Second, the rule will apply to entities that, in many instances, already have obligations to provide notification of data breaches under certain state laws covering medical breaches. Third, once a notice is created, the costs of sending it should be minimal because the Commission anticipates that most consumers will elect to receive notification by e-mail. Nevertheless, to obtain more information about the impact of the proposed rule on small entities, the Commission has decided to publish the following initial regulatory flexibility

analysis pursuant to the Regulatory Flexibility Act, 5 U.S.C. 601-612, as amended, and request public comment on the impact on small businesses of its proposed rule.

A. Description of the Reasons That Action by the Agency is Being Considered

Section 13407 of the American Recovery and Reinvestment Act requires the Commission to promulgate this rule not later than six months after the date of enactment of the Act, or August 18, 2009.

B. Statement of the Objectives of, and Legal Basis for, the Proposed Rule

To implement the requirement that certain entities that handle health information provide notice to individuals whose individually identifiable health information has been breached. The legal basis for the proposed rule is Section 13407 of the American Recovery and Reinvestment Act.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rule Will Apply

The proposed rule will apply to vendors of personal health records, PHR related entities, and third party service providers. As discussed in the section on Paperwork Reduction Act above, FTC staff estimates that the proposed rule will apply to approximately 900 entities. Determining a precise estimate of which of these entities are small entities, or describing those entities further, is not readily feasible. The Commission invites comment and information on this issue.

D. Projected reporting, recordkeeping and other compliance requirements

The Recovery Act and proposed rule impose certain reporting requirements within the meaning of the Paperwork Reduction Act. The Commission is seeking clearance from the Office of Management & Budget (OMB) for these requirements, and the Commission's Supporting Statement submitted as part of that process is being made available on the public record of this rulemaking.

Specifically, the Act and proposed rule require vendors of personal health records and PHR related entities to provide notice to consumers and the Commission in the event of a breach of unsecured PHR identifiable health information. The Act and proposed rule also require third party service providers to provide notice to vendors of personal health records and PHR related entities in the event of such a breach.

If a breach occurs, each entity covered by Act and proposed rule will expend costs to determine the extent of the breach and the individuals affected. If the entity is a vendor of personal health records or PHR related entity, additional costs will include the costs of preparing a breach notice, notifying the Commission, compiling a list of consumers to whom a breach notice must be sent, and sending a breach notice. Such entities may incur additional costs in locating consumers who cannot be reached, and in certain cases, posting a breach notice on a website, notifying consumers through media advertisements, or sending breach notices through press releases to media outlets.

In-house costs may include technical costs to determine the extent of breaches; investigative costs of conducting interviews and gathering information; administrative

costs of compiling address lists; professional/legal costs of drafting the notice; and potentially, costs for postage, web posting, and/or advertising. Costs may also include the purchase of services of a forensic expert.

As noted in the Paperwork Reduction Act analysis above, the estimated annual cost burden for all entities subject to the proposed rule will be approximately $1,020,625. The Commission seeks further comment on the costs and burdens of small entities in complying with the requirements of the proposed rule.

E. Other duplicative, overlapping, or conflicting federal rules.

The FTC has not identified any other federal statutes, rules, or policies currently in effect that would conflict with the proposed rule. As noted above, there is a potential for overlap with forthcoming HHS rules governing breach notification for HIPAA-covered entities. The Commission is consulting with HHS on this potential overlap. The Commission invites comment and information on this overlap, along with any other potentially duplicative, overlapping, or conflicting federal statutes, rules, or policies.

F. Description of any significant alternatives to the proposed rule

In drafting the proposed rule, the Commission has made every effort to avoid unduly burdensome requirements for entities. In particular, the Commission believes that the alternative of providing notice to consumers electronically will assist small entities by significantly reducing the costs of sending breach notices.

The Commission is not aware of alternative methods of compliance that will reduce the impact of the proposed rule on small entities, while also comporting with the Recovery

Act. The statutory requirements are specific as to the timing, method, and content of notice, as well as the effective date of the final rule that results from this Notice of Proposed Rulemaking. Accordingly, the Commission seeks comment and information on ways in which the rule could be modified to reduce any costs or burdens for small entities consistent with the Recovery Act's mandated requirements.

VI. PROPOSED RULE

List of Subjects in 16 CFR Part 318

Consumer protection, Data protection, Health records, Privacy, Trade practices

Accordingly, for the reasons set forth in the preamble, the Commission proposes to add a new Part 318 of title 16 to the Code of Federal Regulations as follows:

PART 318 – HEALTH BREACH NOTIFICATION RULE

Sec.

318.9 Sunset.

Authority: Pub. L. 111-5.

318.1 Purpose and scope.

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 vendors of personal health records, PHR related entities, and third party service providers. 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.

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, any unauthorized acquisition of such information.

(b) Business associate means a business associate under the Health Insurance Portability and Accountability Act, Pub.L. 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, Pub.L. 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 website of a vendor of personal health records;

(2) offers products or services through the websites 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) 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.

(h) 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. If such guidance is not issued by the date specified in section 13402(h)(2), the term "unsecured" shall mean not secured by a technology standard that renders PHR identifiable 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.

(i) 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 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 individual whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, acquired during such breach.

(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 to a vendor of personal health records, PHR related entity, or third party service provider, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such vendor of personal health records, PHR related entity, or third party service provider, respectively) or should reasonably have been known to such vendor of

personal health records, PHR related entity, or third party service provider (or person) to have occurred.

318.4 Timeliness of notification.

(a) In general. Except as provided in paragraph(c) of this section and section 318.5(c), all notifications required under paragraphs 318.3(a) and 318.3(b) shall be made 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 section 164.528(a)(2) of title 45, Code of Federal Regulations, 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 experiences a breach of security shall provide notice of such breach to an individual promptly, as described in section 318.4, and in the following form:

(1) Written notice by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if the individual provides express affirmative consent, by electronic mail. The notice may be provided in one or more mailings as information is available.

(2) 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).

(3) If, after making reasonable efforts to contact the individual through his or her preferred form of communication under paragraph (a)(1), the vendor of personal health records or PHR related entity finds that such preferred form of communication is insufficient or out-of-date, the vendor of personal health records or PHR related entity shall attempt to provide the individual with a substitute form of actual notice, which may include written notice by the consumer's less preferred method or telephone.

(4) If ten or more individuals cannot be reached by the methods specified in paragraphs (a)(1)-(a)(3), the vendor of personal health records or PHR related entity involved shall provide notice:

(i) through a conspicuous posting for a period of six months on the home page of its website; or

(ii) in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside, which shall be reasonably calculated to reach the individuals affected by the breach.

Such a notice in media or web posting shall include a toll-free phone number where an individual can learn whether or not the individual's unsecured PHR identifiable health information may be included in the breach.

(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. Such notice shall include, at a minimum, the information contained in § 318.6.

(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 five business days following the date of discovery of the breach. If the breach involved 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 occurring over the ensuing twelve months and submit the log to the Federal Trade Commission documenting breaches from the preceding year. All notices

pursuant to this paragraph shall be provided according to instructions at the Federal Trade Commission's website.

318.6 Content of notice.

Regardless of the method by which notice is provided to individuals under section 318.5, notice of a breach of security shall include, to the extent possible, the following:

(a) a brief description of how the breach occurred, 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 losses, 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 e-mail address, website, or postal address.

318.7 Enforcement.

A violation of section 318.3 of this Part shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 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 18, 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.

By direction of the Commission.

Donald S. Clark
Secretary