

[Billing Code 6750-01-S]

FEDERAL TRADE COMMISSION

16 CFR Part 318

[RIN 3084-AB17]

Health Breach Notification Rule

AGENCY: Federal Trade Commission (FTC).

ACTION: Final Rule.

SUMMARY: The Federal Trade Commission (“FTC” or “Commission”) is issuing this final rule, as required by the American Recovery and Reinvestment Act of 2009 (the “Recovery Act” or “the Act”). The rule requires vendors of personal health records and related entities to notify consumers when the security of their individually identifiable health information has been breached.

DATES: This rule is effective [insert date 30 days after date of publication in the FEDERAL REGISTER]. Full compliance is required by [insert date 180 days after date of publication in the FEDERAL REGISTER].

ADDRESSES: Requests for copies of the Final Rule and this Notice should be sent to: Public Records Branch, Room 130, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580. The public record of this proceeding is also available at that address. Relevant portions of the proceeding, including the Final Rule and this Notice, are available at www.ftc.gov.

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
- II. Overview of the Recovery Act, Proposed Rule, and Comments Received
- III. Section-By-Section Analysis of the Rule
- IV. Paperwork Reduction Act
- V. Regulatory Flexibility Act
- VI. Final Rule

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.¹ 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 vendors of personal health records and online applications that interact with such personal health records (“PHRs”).² Some of these entities are not subject to the existing

¹ American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

² In general, personal health records are online repositories of health information that individuals can create to track their medical visits, prescription information, etc. 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 to submit a report to Congress containing recommendations within one year of enactment of the Recovery Act (the “HHS report”). Until Congress enacts new legislation implementing such recommendations, the Recovery Act contains temporary requirements, to be enforced by the FTC, that such entities notify individuals in the event of a security breach. The final rule implements these requirements.

The Recovery Act also directs HHS to promulgate a rule 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 HIPAA-covered entities in the event of a security breach.⁴ HIPAA-covered entities and entities that engage in activities as business associates of HIPAA-covered entities will be subject only to HHS’ rule and not the FTC’s rule, as explained further below.

terms “vendor of personal health records” and “personal health records” are defined terms in the FTC’s rule; thus, in some instances, the term “personal health record” is not abbreviated.

³ Health Insurance Portability & Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

⁴ The Recovery Act requires HHS to issue its rule within 180 days of enactment of the Recovery Act. Sec. 13402(j).

II. Overview of the Recovery Act, Proposed Rule, and Comments Received

The Recovery Act requires “vendors of personal health records” and “PHR related entities,” as defined below, to notify their customers of any breach of unsecured, individually identifiable health information. Further, a third party service provider of such vendors or entities that experiences a breach must notify such vendors or entities of the breach, so that they can in turn notify their customers. The Act contains specific requirements governing the timing, method, and contents of the breach notice to consumers. For example, it requires entities to provide breach notices “without unreasonable delay,” and in no case later than 60 calendar days after discovering a breach; it requires notice to consumers by first-class mail or, if specified as a preference by the individual, by email; and it requires substitute notice, through the media or a web posting, if there is insufficient contact information for ten or more individuals. In addition, the Act requires the FTC to adopt a rule implementing the breach notification requirements applicable to vendors of personal health records, PHR related entities, and third party service providers within 180 days of enactment of the Act. It also authorizes the FTC to seek civil penalties for violations.

The Recovery Act contains a similar scheme for HIPAA-covered entities, to be enforced by HHS. HIPAA-covered entities must notify individuals whose “unsecured protected health information” is breached. If a business associate of a HIPAA-covered entity experiences a security breach, it must notify the HIPAA-covered entity, which must in turn notify individuals.

To fulfill the Recovery Act requirements, on April 20, 2009, the Commission issued a Notice of Proposed Rulemaking (“NPRM”). The proposed rule contained in the NPRM adhered closely to the requirements of the Recovery Act.⁵ The Commission received approximately 130 comments.⁶ Some general comments are summarized below, and an analysis of comments addressing particular sections of the proposed rule follows.

First, commenters that addressed the issue generally agreed that FTC and HHS should work together to ensure that their respective breach notification rules are harmonized and that stakeholders know which rule applies to which entity.⁷ Some of these commenters recognized that some entities that operate in different roles may be subject to both rules, and that it is therefore important for the rules to be similar.⁸ The Commission agrees and has consulted with HHS to harmonize the two rules, within the constraints of the statutory language. Further, as explained below, for some entities

⁵ 74 FR 17,914.

⁶ Comments are available at <http://www.ftc.gov/os/comments/healthinfobreach/index.shtm>. The Commission also reviewed the comments HHS received in response to its Request for Information on its forthcoming breach notification rule. 74 FR 19,006. However, the specific comments addressed in this Notice are those that were filed in response to the FTC’s NPRM.

⁷ *See, e.g.*, American Council of Life Insurers (“ACLI”) at 1; American Benefits Council (“ABC”) at 2; American Insurance Association (“AIA”) at 1; Center for Democracy & Technology, Markle Foundation, Childbirth Connection, Health Care for All, National Partnership for Women & Families, SEIU (hereinafter “CDT/Markle”) at 4-5; Dossia at 5; HealthITNow.org at 1-2; National Association of Chain Drug Stores (“NACDS”) at 4; WebMD at 3.

⁸ *See, e.g.*, HealthITNow.org at 2; WebMD at 3.

subject to both the HHS and FTC rules, compliance with certain HHS rule requirements shall be deemed compliance with the corresponding provisions of the FTC's rule.

A second and related point that many commenters raised was that, to the extent possible, consumers should receive a single notice for a single breach.⁹ These commenters pointed out that receiving multiple notices for the same breach would confuse consumers and convey an exaggerated sense of risk.¹⁰ Receiving a barrage of notices also could cause consumers to become numb to such notices, so that they may fail to spot or mitigate the risks being communicated to them.¹¹ Some commenters noted that consumers could receive multiple notices because of inadvertently overlapping requirements between HHS and FTC rules.¹² As described below, the Commission has taken steps to ensure that its rule does not overlap with HHS' and that consumers do not receive multiple notifications.

Third, several commenters raised privacy and security concerns about PHRs generally.¹³ For example, one commenter asked the FTC to establish comprehensive privacy and security standards, and supported the creation of a private right of action for

⁹ *See, e.g.*, American Legislative Exchange Council (“ALEC”) at 6; HealthITNow.org at 2; Software Information Industry Association (“SIIA”) at 3; Statewide Parent Advocacy Network, Inc. at 1; United Health Group (“UHG”) at 2.

¹⁰ *See, e.g.*, ALEC at 7; HealthITNow.org at 2.

¹¹ *See, e.g.*, Blue Cross/Blue Shield at 4; SIIA at 6-7.

¹² *See, e.g.*, American Health Information Management Association (“AHIMA”) at 2; American Medical Association (“AMA”) at 2.

¹³ *See, e.g.*, Electronic Privacy Information Center (“EPIC”) at 11; Flagler, Hoerl, Hosler.

a violation of these standards.¹⁴ The Commission notes that, although general privacy and security issues are beyond the scope of the current rulemaking, the Commission will take these comments into account when it provides input on the HHS report described above.

Fourth, several individual commenters expressed concerns about electronic health records in general.¹⁵ Some of these commenters questioned the cost-savings that would result;¹⁶ others strongly supported patients' right to opt out of such records.¹⁷ In response, the Commission notes that this rule addresses only breach notification with respect to PHRs voluntarily created by individuals; it does not address electronic health records more generally, such as those created for patients by hospitals or doctors' offices.¹⁸

Finally, many commenters expressed concerns about particular statutory requirements governing breach notification. For example, some commenters stated that entities should be required to provide breach notification for paper, as well as electronic,

¹⁴ EPIC at 11.

¹⁵ *See, e.g.*, Blair, Coon, Flagler.

¹⁶ *See, e.g.*, Jones-Ford, Rogalski, Serich,

¹⁷ *See, e.g.*, Amidei, Baxter, Blair, Coon.

¹⁸ Section 13400(5) of the Recovery Act defines "electronic health record" as an electronic record of health-related information on an individual that is "created, gathered, managed, and consulted by authorized health care clinicians and staff." In contrast, section 13400(11) defines "personal health record" as an electronic record "on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."

information;¹⁹ others expressed concerns about requiring media notice.²⁰ Because these requirements come directly from the language of the Recovery Act, the Commission cannot change its final rule in response to these comments. Nevertheless, the Commission will take these comments into account when it provides input on the HHS report.

III. Section-by-Section Analysis

Section 318.1: Purpose and Scope

Proposed section 318.1 set forth the relevant statutory authority for the proposed rule; stated that the proposed rule would apply to vendors of personal health records, PHR related entities, and third party service providers; and clarified that the proposed rule would not apply to HIPAA-covered entities or to an entity's activities as a business associate of a HIPAA-covered entity. The Commission received several comments on this section as follows.

A. Application of Rule to Non-Profits and Other Entities Beyond the FTC's Traditional Jurisdiction

In its NPRM, the Commission noted that the proposed rule applied to entities beyond the FTC's traditional jurisdiction under section 5 of the FTC Act, such as non-profits (e.g., educational institutions, charities, and 501(c)(3) organizations), because the Recovery Act does not limit the FTC's enforcement authority to its enforcement

¹⁹ See, e.g., IDEXperts at 1-2; National Association for Information Destruction ("NAID") at 3-4, Ohio State University Medical Center at 1, Statewide Parent Advocacy Network, Inc. at 2.

²⁰ See, e.g., IDEXperts at 2-3; Identity Theft 911 at 3.

jurisdiction under section 5. Indeed, section 13407 of the Recovery Act expressly applies to “vendors of personal health records and other non-HIPAA covered entities,” without regard to whether such entities fall within the FTC’s jurisdiction under section 5.

The Commission received several comments in support of this requirement. One commenter stated that it was reasonable for the FTC’s rule to apply to non-profits.²¹ Another commenter suggested applying the rule to as broad a range of entities as possible.²² Yet another commenter stated that the rule should apply to all entities that handle PHRs.²³ Thus, the Commission retains its interpretation and modifies the proposed rule to clarify that it applies to vendors of personal health records and PHR related entities, “irrespective of any jurisdictional tests in the Federal Trade Commission Act.”²⁴

B. Application of the FTC’s Rule to HIPAA-Covered Entities and Business Associates of HIPAA-Covered Entities

As noted above, the Commission received many comments about the need to harmonize the HHS and FTC rules to simplify compliance burdens and create a level-playing field for HIPAA and non-HIPAA covered entities.²⁵ Several commenters agreed

²¹ CDT/Markle at 14-15.

²² IDEXperts at 1.

²³ *See, e.g.*, EPIC at 3.

²⁴ The rule will not apply to federal agencies. The Commission notes that federal agencies already follow breach reporting requirements established by the Office of Management and Budget (“OMB”). *See* OMB Memorandum for the Heads of Executive Departments and Agencies re Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007, *available at* <http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf>.

²⁵ *See supra* note 7.

with the statements in the FTC’s NPRM that (1) HIPAA-covered entities should be subject to HHS’ breach notification rule and not the FTC’s rule; and (2) business associates of HIPAA-covered entities should be subject to HHS’ breach notification rule, but only to the extent they are acting as business associates.²⁶ Accordingly, the FTC adopts as final the provision that the rule “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,” but provides further guidance in response to specific comments received on the issue.

1. Application of the FTC’s Rule to HIPAA-Covered Entities

Although the FTC’s proposed rule made clear that it did not apply to HIPAA-covered entities, one medical association urged the Commission to exclude doctors explicitly from the FTC rule, even if they are involved with PHRs.²⁷ The Commission agrees that, because health care providers such as doctors are generally HIPAA-covered entities, the FTC’s rule does not apply to them in such capacity. Thus, if a doctor’s medical practice offers PHRs to its patients, neither the doctor nor the medical practice is subject to the FTC’s rule.²⁸ However, if the doctor creates a PHR in a personal capacity,

²⁶ *See, e.g.*, Dossia at 5; UHG at 2; WebMD at 2.

²⁷ American Medical Association at 1-2.

²⁸ Some doctors or other health care providers, however, may not be HIPAA-covered entities because they do not participate in “covered transactions” under HIPAA regulations, such as submitting health care claims to a health plan. *See* 45 CFR 160.103. In such cases, these doctors or health care providers are subject to the FTC’s rule if they offer PHRs or related services. Similarly, some commenters asked whether the FTC’s rule applies to education records covered by the Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. 1232g (i.e., records of educational institutions such as public schools and universities). *See* Ohio State University Medical Center at 1; Statewide

there may be circumstances under which the FTC's rule would apply. For example, a non-practicing doctor may create and offer PHRs to the public as part of a start-up business venture. In this circumstance, the doctor is not acting in his or her capacity as a HIPAA-covered entity, and thus, the FTC's rule would regulate the PHRs.

In addition, one commenter asked whether the FTC's rule would cover PHRs that a HIPAA-covered entity offers to its employees.²⁹ Because the FTC's rule does not apply to HIPAA-covered entities, it does not apply to PHRs that such entities offer their employees. However, if a HIPAA-covered health care provider or group health plan offers PHRs to employees because they also are patients of such health care provider or enrollees of such group health plan, then HHS' rule would apply to the PHRs.

2. Application of the FTC's Rule to Business Associates of HIPAA-Covered Entities

In its NPRM, the Commission recognized that, in many cases, business associates of HIPAA-covered entities that also offer PHRs to the public could be subject to both the HHS and FTC breach notification rules. If they experience a breach, they could be required to provide direct breach notification to their individual customers under the FTC's rule. At the same time, under HHS' rule, they could be required to notify HIPAA-covered entities to whom they provide services, so that the HIPAA-covered entities could in turn notify individuals. In some cases, as discussed further below, this potential overlap could lead to consumers' receiving multiple notices for the same breach.

Parent Advocacy Network at 3-4. If school nurses or physicians' offices within these institutions are not HIPAA-covered entities, they are subject to the FTC's rule if they offer PHRs or related services.

²⁹ Ohio State University Medical Center at 1.

The Commission asked for examples of vendors of personal health records that may have a dual role as a business associate of a HIPAA-covered entity and as a direct provider of PHRs to the public, and how the rule should address such a dual role. Commenters provided several useful examples,³⁰ all of which the Commission believes can be addressed within the framework provided in the rule. Most commenters that addressed the issue stated, and the Commission agrees, that regardless of the circumstances, consumers should receive a single breach notice for a single breach.³¹ In addition, the Commission agrees with the commenters that stated that the breach notice should come from the entity with whom the consumer has a direct relationship.³² Indeed, the Commission believes that consumers are more likely to pay attention to a notice provided by an entity known to the consumer, and that consumers may ignore or discard notices provided by unknown entities.³³

For these reasons, it may be desirable in some circumstances for a vendor of personal health records to provide notice directly to consumers even when the vendor is serving as a business associate of a HIPAA-covered entity. For example, a consumer that obtained a PHR through a HIPAA-covered entity may nevertheless deal directly with the PHR vendor in managing his or her PHR account, and would expect any breach notice to

³⁰ *See, e.g.*, Dossia at 2-3; UHG at 3; WebMD at 3.

³¹ *See supra* note 9.

³² *See, e.g.*, CDT/Markle at 12; Dossia at 5.

³³ *See, e.g.*, Statement of Basis and Purpose, Affiliate Marketing Rule, 72 FR 62910 (Nov. 7, 2007) (requiring that opt-out notices come from entity with whom the consumer has a relationship).

come from the PHR vendor. Similarly, where a vendor of personal health records has direct customers and thus is subject to the FTC’s rule, and also provides PHRs to customers of a HIPAA-covered entity through a business associate arrangement, it may be appropriate for the vendor to provide the same notice to all such customers. In the latter situation, the Commission believes that the vendor of personal health records should be able to comply with one set of rule requirements – those promulgated by HHS – governing the timing, method, and content of notice to consumers. Thus, in those limited circumstances where a vendor of personal health records (1) provides notice to individuals on behalf of a HIPAA-covered entity, (2) has dealt directly with these individuals in managing the PHR account, and (3) provides such notice at the same time that it provides an FTC-mandated notice to its direct customers for the same breach, the FTC will deem compliance with HHS requirements governing the timing, method, and content of notice to be compliance with the corresponding FTC rule provisions.³⁴

Based on the comments received, the Commission has developed the following examples to illustrate situations of dual or overlapping coverage under the FTC and HHS rules.

a. Example 1: Vendor with a Dual Role as Business Associate and Provider of PHRs to the Public

PHR Vendor provides PHRs to the public through its own website. PHR Vendor also signs a business associate agreement with ABC Insurance (a HIPAA-covered entity)

³⁴ For direct customers, the vendor of personal health records still must comply with all other FTC rule requirements, including the requirement to notify the FTC within ten business days after discovering the breach. The Commission notes also that the above analysis would apply equally to a PHR related entity, as defined below, that deals directly with the public and acts as a business associate in providing services.

to offer PHRs to customers of ABC Insurance. ABC Insurance sends a message to its customers offering free PHRs through PHR Vendor and provides a link to PHR Vendor's website. Several patients of ABC Insurance choose to create PHRs through PHR Vendor. A hacker remotely copies the PHRs of all of PHR Vendor's users.

Under the FTC's rule, PHR Vendor is a vendor of personal health records that must provide breach notice to members of the public to whom it offers PHRs directly. It is not acting as a business associate to anyone in providing these PHRs. However, because it is acting as a business associate to ABC Insurance by providing PHRs for ABC Insurance's patients, it is not required to provide direct notice to ABC Insurance's customers under the FTC's rule. Rather, under the Recovery Act, in its capacity as a business associate, it must notify ABC Insurance so that ABC Insurance can in turn notify its customers.

PHR Vendor therefore must maintain a list of its own customers and a separate list of ABC Insurance's customers so that it can fulfill its obligations under the Recovery Act to provide notice to its own customers, as well as a separate notice to ABC Insurance. If PHR Vendor has similar business associate agreements with other entities, it must maintain separate customer lists for each such entity.

In this example, however, because PHR Vendor has a direct relationship with all of the individuals affected by the breach (including the patients of ABC Insurance), PHR Vendor may contract with ABC Insurance to notify individuals on ABC Insurance's

behalf.³⁵ The Commission encourages such contractual arrangements because they would (1) satisfy both PHR Vendor's and ABC Insurance's obligation to notify individuals; (2) ensure that consumers receive a single notice from an entity with whom they have a direct relationship; and (3) simplify the notification process so that PHR Vendor can provide direct notice to those affected at the same time.³⁶

b. Example 2: Addressing Portable PHRs

As in Example 1, PHR Vendor offers PHRs directly to the public. It also offers PHRs to enrollees of various health insurance companies, including ABC Insurance and XYZ Insurance, through business associate agreements with those companies. Sally is a patient of ABC Insurance. ABC Insurance offers Sally the use of PHR Vendor's product, and Sally creates her PHR. Years later, Sally moves, changes jobs, switches to XYZ Insurance, and keeps her PHR with PHR Vendor. If PHR Vendor's records are breached at this point, under HHS' rule, PHR Vendor, as a business associate of XYZ Insurance, must notify XYZ Insurance that Sally's record has been breached, and XYZ Insurance must provide Sally with a breach notice. Alternatively, if Sally had moved to an insurance company with whom PHR Vendor did not have a business associate agreement, PHR Vendor would not be subject to HHS' rule with respect to Sally; it must treat her as its own customer and provide Sally with breach notice directly.

³⁵ PHR Vendor still must comply with the Recovery Act requirement to notify ABC Insurance of the breach.

³⁶ As explained above, if PHR Vendor were to send individual notices on behalf of ABC Insurance, it could send all of its breach notices, including notices to its direct customers, in accordance with HHS rules requirements governing the timing, method, and content of notice.

In this scenario, PHR Vendor has an additional obligation to address the potential portability of PHRs. To fulfill such obligation, PHR Vendor must maintain lists tracking which customers belong to which HIPAA-covered entity, and must update such information regularly. Without such an updating system, PHR Vendor might keep Sally on its list of ABC Insurance's customers, but when Sally leaves ABC Insurance, that company may no longer have an obligation to notify her of a breach, and she may never receive a notice.³⁷ Alternatively, if PHR Vendor does not properly update its customer lists, Sally potentially could receive up to three notices – one from PHR Vendor, one from ABC Insurance, and one from XYZ Insurance.

As in Example 1, the Commission encourages vendors like PHR Vendor to include provisions in their business associate agreements stating that they will send breach notices on behalf of the entities to whom they are providing business associate services. In Example 2, such a contractual provision would simplify the notification process; it also may help avoid a situation in which consumers like Sally, who may move around frequently, receive multiple notices, or even worse, no notice.

c. Example 3: PHRs Offered to Families

Sally is employed by ABC Widgets, which has a HIPAA-covered group health plan. ABC Widgets' group health plan offers PHRs to employees and employees' spouses through PHR Vending, a business associate of ABC Widgets' group health plan. Sally gets a PHR; her husband John is separately insured, but he decides to get a PHR

³⁷ PHR Vendor's failure to send Sally a notice in this situation would constitute a violation of the FTC's rule.

through PHR Vending as well. If PHR Vending experiences a breach, Sally may get a notice from ABC Widgets' group health plan under HHS' rule, and John must get a notice from PHR Vending under the FTC's rule. Alternatively, ABC Widgets and PHR Vending may, through their business associate agreement, choose to have PHR Vending send breach notices to all customers, as explained above.

C. Application of the FTC's Rule to Entities Outside the United States

One commenter suggested that the Commission clarify whether its rule applies to foreign businesses that have U.S. customers.³⁸ The Commission agrees and has determined that foreign entities with U.S. customers must provide breach notification under U.S. laws. Accordingly, it adds language to the final rule stating that it “applies to foreign and domestic vendors of personal health records, PHR related entities, and third party service providers . . . that maintain information of U.S. citizens or residents.”

The Recovery Act supports this interpretation. Section 13407(e) of the Act states that a violation of the FTC's breach notification provisions “shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act . . .” Section 18(a)(1)(B) allows the Commission to issue regulations that define “with specificity acts or practices which are unfair or deceptive acts or practices” under the FTC Act.³⁹ The term “unfair or deceptive acts or practices” is in turn defined to include those acts or practices “in foreign commerce” that “cause or are likely to cause reasonably foreseeable injury within the United States” or “involve

³⁸ World Privacy Forum at 1-2.

³⁹ 15 U.S.C. 57a.

material conduct occurring within the United States.”⁴⁰ Thus, the Recovery Act’s references to the “unfair or deceptive acts or practices” section of the FTC Act, which has extraterritorial reach, supports the interpretation that the FTC’s rule applies to foreign vendors of personal health records, related entities, as well as third party service providers, to the extent that they deal with U.S. consumers.

D. Preemption of State Law

Several commenters discussed state breach notification requirements that could potentially conflict with the FTC’s rule requirements.⁴¹ Several of these commenters raised concerns that such conflicting requirements could increase compliance burdens on businesses.⁴² Some also raised concerns that entities would be required to send consumers multiple notices to comply with both state laws and the FTC’s rule.⁴³

The Commission notes that, under section 13421 of the Recovery Act, the preemption standard set forth in section 1178 of the Social Security Act, 42 U.S.C. 1320d-7 applies also to the FTC’s rule. That section, which contains the preemption standard for HIPAA and its implementing regulations, states that federal requirements

⁴⁰ 15 U.S.C. 45.

⁴¹ *See, e.g.*, America’s Health Insurance Plans (“AHIP”) at 7; AIA at 1; Dossia at 10-11; Molina Healthcare at 5-6; NACDS at 3-4; National Association of Mutual Insurance Companies (“NAMIC”) at 7-8; SIIA at 2-3; Sonnenschein at 1-2; UHG at 9-12; WebMD at 5-7.

⁴² *See, e.g.*, AIA at 1; Dossia at 10; Molina Healthcare at 5-6.

⁴³ *See, e.g.*, AHIP at 8; AIA at 2.

supersede any contrary provision of State law.⁴⁴ To clarify that the same standard applies here, the Commission has added language to the final rule stating that, “[t]his Part preempts state law as set forth in section 13421 of the American Recovery and Reinvestment Act of 2009.”

The Commission notes that the final rule preempts only *contrary* state laws. Under HHS regulations implementing the preemption standard of section 1178 of the Social Security Act, a state law is contrary to federal requirements (1) if it would be impossible to comply with both state and federal requirements or (2) if state law “stands as an obstacle to the accomplishment and execution of the full purposes and objectives” of the federal requirements.⁴⁵ Under this standard, the Commission’s rule does not preempt state laws imposing additional, as opposed to contradictory, breach notification requirements. For example, some state laws require breach notices to include advice on monitoring credit reports; others require contact information for consumer reporting agencies; yet others require the notice to include advice on reporting incidents to law enforcement agencies. Even though these content requirements are different from those contained in the FTC’s rule, entities may comply with both state laws and the FTC rule

⁴⁴ Section 1178 also sets forth some exceptions to this standard, none of which applies here. Of most relevance, one exception states that federal requirements will not necessarily preempt contrary state laws that, “subject to section 264(c)(2)” of HIPAA, relate to the “privacy of individually identifiable health information.” Although the FTC’s rule relates to “privacy of individually identifiable health information,” HHS interprets this exception as applying only to the HIPAA Privacy Rule, because it is the sole regulation promulgated under section 264(c)(2) of HIPAA.

⁴⁵ See 45 CFR 160.202.

by setting forth all of the information required in a single breach notice.⁴⁶ In these circumstances, because it is possible to comply with both laws, and the state laws do not thwart the objectives of the federal law,⁴⁷ there is no conflict between state and federal law.

Section 318.2: Definitions

(a) Breach of security

The proposed rule defined “breach of security” as the acquisition of unsecured PHR identifiable health information⁴⁸ of an individual in a personal health record without the authorization of the individual.⁴⁹ The Commission adopts this portion of the definition of breach of security without modification. Examples of unauthorized acquisition include the theft of a laptop containing unsecured PHRs; 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.

The proposed rule also contained a rebuttable presumption for unauthorized *access* to an individual’s data: It stated that, when there is unauthorized access to data, unauthorized acquisition will be presumed unless the entity that experienced the breach

⁴⁶ The rule does not require entities to send multiple notices to comply with state and federal law.

⁴⁷ For a discussion of the issue of federal preemption when state laws frustrate federal objectives, *see Wyeth v. Levine*, 129 S. Ct. 1187 (2009).

⁴⁸ The phrase “PHR identifiable health information” is defined below.

⁴⁹ Several of the rule provisions refer to information “in a personal health record.” Because a personal health record often includes information in transit, as well as stored information, the Commission interprets the phrase “in a personal health record” to include data in motion and data at rest.

“has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.” The presumption was intended to address the difficulty of determining whether access to data (i.e., the opportunity to view the data) did or did not lead to acquisition (i.e., the actual viewing or reading of the data). In these situations, the Commission stated that the entity that experienced the breach is in the best position to determine whether unauthorized acquisition has taken place.

In describing the rebuttable presumption, the Commission provided several examples. It noted that no breach of security has occurred if an unauthorized employee inadvertently accesses an individual’s PHR and logs off without reading, using, or disclosing anything. If the unauthorized employee read the data and/or shared it, however, he or she “acquired” the information, thus triggering the notification obligation in the rule.

Similarly, the Commission provided an example of a lost laptop: If an entity’s employee loses a laptop 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, for example, that the laptop was recovered, and that forensic analysis revealed that files were never opened, altered, transferred, or otherwise compromised.

The Commission received numerous comments on the rebuttable presumption. Several commenters supported it.⁵⁰ Others stated that the standard articulated by the Commission is too broad and instead should require breach notification only when there

⁵⁰ See, e.g., AHIMA at 3; IDEXperts at 1; NAID at 2; NAMIC at 3; Statewide Parent Advocacy Network, Inc., at 2, World Privacy Forum at 6-7.

is a risk of harm.⁵¹ Several of these commenters stated that the Commission’s proposed standard would result in consumers’ being inundated with breach notices.⁵² In contrast, consumer groups expressed concern that the Commission was giving too much discretion to companies, which could easily claim that unauthorized access did not give rise to unauthorized acquisition.⁵³ Several commenters also requested further guidance on how the rebuttable presumption would work in specific instances.⁵⁴

After considering the comments received, the Commission has decided to adopt the rebuttable presumption as part of the definition of breach of security, without modification. In response to the comments suggesting that the Commission require notification only if there is a risk of harm, the Commission notes that its standard does take harm into account. Indeed, notification would not be required in a case where an entity can show that although an unauthorized employee accidentally opened a file, it was not viewed, and therefore there has been no harm to the consumer.

The Commission notes that harm in the context of health information may be different from harm in the context of financial information. As one commenter stated, “[w]ith a breach of financial records, a consumer faces a significant headache, but ultimately can have their credit and funds restored; this is not the case with health records. A stigmatizing diagnosis, condition or prescription in the wrong hands can

⁵¹ *See, e.g.*, AIA at 2, Blue Cross/Blue Shield at 3; National Community Pharmacists Association at 2; SIIA at 4-7; UHG at 3-5; WebMD at 4.

⁵² *See, e.g.*, Blue Cross/Blue Shield at 4; SIIA at 6-7.

⁵³ *See, e.g.*, CDT/Markle at 8-9; EPIC at 5.

⁵⁴ *See, e.g.*, AHIP at 2; IDEXperts at 1; Intuit at 2; Molina Healthcare at 2.

cause irreversible damage and discrimination.”⁵⁵ Because health information is so sensitive, the Commission believes the standard for notification must give companies the appropriate incentive to implement policies to safeguard such highly-sensitive information.

With respect to commenters’ concerns about the possibility of consumers’ being inundated with breach notifications, the Commission believes that its standard strikes the right balance. Given the highly personal nature of health information, the Commission believes that consumers would want to know if such information was read or shared without authorization. In addition, the danger of overnotification may be overstated. For example, where there has been unauthorized access to a database leading to the acquisition of specific consumers’ data, a vendor or entity need not notify all consumers whose information appears in that database; it only needs to notify those specific consumers whose data was acquired.

Nevertheless, the Commission agrees that further guidance would be useful to entities in assessing whether unauthorized acquisition has taken place as a result of unauthorized access. This further guidance should also allay consumer groups’ concerns that businesses have too much discretion in making this determination. Commenters posed several scenarios, which the Commission addresses here.

First, one commenter noted that companies should not have to delve into the state of mind of employees who accessed data to determine whether they viewed, read,

⁵⁵ *See Patient Privacy Rights* at 6.

memorized, or shared such data.⁵⁶ The Commission agrees and notes that, in a case of inadvertent access by an employee, no breach notification is required if (1) the employee follows company policies by reporting such access to his or her supervisor and affirming that he or she did not read or share the data, and (2) the company conducts a reasonable investigation to corroborate the employee's version of events.

Second, some commenters asked if unauthorized acquisition has taken place when a PHR is accessible on the Internet through an obscure website.⁵⁷ The Commission believes that it would be very difficult to overcome the presumption that unauthorized acquisition has taken place in this scenario. In fact, because the Internet is accessible to hundreds of millions of people around the world, it is not generally reasonable to assume that the information available on the Internet was not acquired. The presumption of unauthorized acquisition could likely only be overcome if there was forensic evidence showing that the page was not viewed.

Third, and similar to the example above, if an employee sends a mass email containing an individual's unsecured PHR identifiable health information accidentally, and the employee immediately recalls the message, the Commission believes that it is highly unlikely that the presumption can be overcome. In contrast to a situation in which an employee sends a single email and immediately asks the recipient to delete it, once

⁵⁶ *See, e.g.*, SIIA at 5.

⁵⁷ *See* NAID at 2; Patient Privacy Rights at 4-5.

hundreds of people have received an email, the Commission does not believe that there can be a reasonable expectation that no one “acquired” the information.⁵⁸

On a related issue, the final rule provides that a breach of security means acquisition of information without the authorization “of the individual.” Some commenters raised questions about how the extent of individual authorization should be determined.⁵⁹ For example, if a privacy policy contains buried disclosures describing extensive dissemination of consumers’ data, could consumers be said to have authorized such dissemination?

The Commission believes that an entity’s use of information to enhance individuals’ experience with their PHR would be within the scope of the individuals’ authorization, as long as such use is consistent with the entity’s disclosures and individuals’ reasonable expectations. Such authorized uses could include communication of information to the consumer, data processing, or Web design, either in-house or through the use of service providers. Beyond such uses, the Commission expects that vendors of personal health records and PHR related entities would limit the sharing of consumers’ information, unless the consumers exercise meaningful choice in consenting to such sharing. Buried disclosures in lengthy privacy policies do not satisfy the standard

⁵⁸ *See In the Matter of Eli Lilly & Co.*, Docket No. C-4047 (May 8, 2002) (settlement of action in which FTC alleged that company failed to maintain reasonable security; employee inadvertently had sent mass email revealing customers’ sensitive health information).

⁵⁹ *See, e.g.*, CDT/Markle at 10; International Pharmaceutical Privacy Consortium at 2; SIIA at 6.

of “meaningful choice.”⁶⁰ The Commission will examine this issue further when providing input on the HHS report.

(b) Business associates and (c) HIPAA-covered entities

Proposed paragraph (b) defined “business associate” to mean a business associate under HIPAA, as defined in 45 C.F.R 160.103. That regulation, in relevant part, defines a business associate as an entity that handles the protected health information of a HIPAA-covered entity and (1) provides certain functions or activities on behalf of the HIPAA-covered entity or (2) provides “legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for” the HIPAA-covered entity. Proposed paragraph (c) defined “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

⁶⁰ See, e.g., *In the Matter of Sears Management Holding Co.*, File No. 082 3099 (June 4, 2009) (accepted for public comment) (alleging that Sears’ failure to adequately disclose its tracking activities violated the FTC Act, given that Sears only disclosed such tracking in a lengthy user license agreement, available to consumers at the end of a multi-step registration process); FTC Staff Report, “Self-Regulatory Principles for Online Behavioral Advertising,” Feb. 2009, <http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf>; FTC Publication, *Dot Com Disclosures: Information About Online Advertising* at 5 (May 2000), available at <http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf> (“Making [a] disclosure available . . . so that consumers who are looking for the information *might* find it doesn’t meet the clear and conspicuous standard . . . [D]isclosures must be communicated effectively so that consumers are likely to notice and understand them.”) (emphasis in original); see also FTC Policy Statement on Deception, appended to *In the Matter of Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), available at <http://www.ftc.gov/bcp/policystmt/ad-decept.htm> (fine print disclosures not adequate to cure deception).

processing services for health information), or a health plan. The Commission adopts these definitions without modification.

(d) Personal health record

Proposed paragraph (d) defined 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.” The FTC adopts this definition without modification.⁶¹

Several commenters urged the FTC to cover paper records, as well as electronic records.⁶² Although the Commission agrees that breaches of data in paper form can be as harmful as breaches of such data in electronic form, the plain language of the Recovery Act compels the Commission to issue a rule covering only electronic data.⁶³ The Commission will examine this issue further when providing input on the HHS report to Congress.

⁶¹ In response to comments received, the Commission emphasizes that PHRs are managed, shared, and controlled “by or primarily for the individual.” *See, e.g.*, AIA at 2; ACLI; Molina Healthcare at 2-3; National Association of Mutual Insurance Companies (“NAMIC”) at 3-4. Thus, they do not include the kinds of records managed by or primarily for commercial enterprises, such as life insurance companies that maintain such records for their own business purposes.

⁶² *See supra* note 19.

⁶³ *See Pinero v. Jackson Hewitt Tax Service, Inc.*, 594 F. Supp. 2d 710, 716-17 (E.D. La. 2009) (dismissing plaintiff’s claim alleging breach of paper records under Louisiana data breach notification law because that law covers only a breach of “computerized” data).

(e) PHR identifiable health information

Proposed paragraph (e) defined “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)),⁶⁴ 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.” The Commission adopts this definition without change.

In its NPRM, the Commission noted three points with respect to this definition. First, it stated that the definition of “PHR identifiable health information” includes *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.⁶⁵ The Commission retains this interpretation.

Second, the Commission noted that the proposed rule would cover a security breach of a database containing names and credit card information, even if no other information was included. Several commenters pointed out that this approach was not supported by the statutory language of the Recovery Act, which defines “PHR

⁶⁴ 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.”

⁶⁵ 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 breach notification, even if no specific health information is contained in that list.

identifiable health information” to include information that relates to payment only “for the provision of health care to an individual.” These commenters noted that providing PHRs to consumers does not constitute the “provision of health care to an individual.”⁶⁶ The Commission is persuaded that name and credit card information alone is not PHR identifiable health information. However, as noted above, if the disclosure of credit card information identifies an individual as a customer of a vendor of personal health records or related entity associated with a particular health condition, that information would constitute “PHR identifiable health information.”⁶⁷

Third, the Commission stated that, 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 breach notification need not be provided. The Commission also stated that, if a breach involves information that has been “de-identified” under 45 CFR 164.514(b),⁶⁸ the Commission will deem that information to fall outside the scope of “PHR identifiable health information” and therefore not covered by the rule. 45 CFR 164.514(b) states that data is “de-identified” (1) if there has been a formal, documented analysis by a qualified statistician that the risk of re-identifying the individual associated with such data is “very small,” or (2) if specific identifiers about the individual, the individual’s relatives, household members, and employers (including

⁶⁶ See, e.g., Intuit at 2; MasterCard at 1-3; SIIA at 10, Dossia at 6-7.

⁶⁷ The Commission also notes that, depending on the circumstances, the failure to secure name and credit card information could constitute a violation of section 5 of the FTC Act. See http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

⁶⁸ This standard, which appears in the HIPAA Privacy Rule, creates an exemption to that Rule.

names, contact information, birth date, and zip code) are removed, and the covered entity has no actual knowledge that the remaining data could be used to identify the individual. The Commission also requested examples of other 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 received numerous comments on this issue. Some commenters supported the Commission’s proposal that “de-identified” data not be deemed “PHR identifiable health information.”⁶⁹ Others rejected this standard as not sufficiently protective of consumers because, in some instances, even “de-identified” data can be tracked back to an individual.⁷⁰

One commenter requested that the FTC similarly state that “limited data sets” under HIPAA are not “PHR identifiable health information.”⁷¹ Under HIPAA’s Privacy Rule, HIPAA-covered entities may use “limited data sets” for research, public health, or health care operations without individual authorization, as long as contracts govern the use of such data. “Limited data sets” do not include names, addresses, or account numbers; they can, however, include an individual’s city, town, five-digit zip code, and date of birth.⁷² Another commenter urged the FTC to state that, if information has been

⁶⁹ *See, e.g.*, Columbia University at 2; NACDS at 2.

⁷⁰ CDT/Markle at 7-8; EPIC at 6-8; Patient Privacy Rights at 5-6.

⁷¹ Minnesota Department of Health at 3.

⁷² 45 CFR 164.514(e). De-identified data sets cannot contain even this information, unless a qualified statistician determines that such information, when combined with other data, would present a “very small” risk of re-identification.

“redacted, truncated, obfuscated, or otherwise pseudonymized,” there is no reasonable basis to believe that the information can be used to identify the individual.⁷³ Indeed, several commenters noted that mandating notification for breaches of data that does not include individual identifiers would require re-identification of individuals associated with such data, the process of which would expose their information to new security risks.⁷⁴

With respect to “de-identified” data and “limited data sets,” commenters provided empirical evidence on the likelihood that such data could be combined with other data to identify individuals. For example, several commenters cited to the research of Dr. LaTanya Sweeney of Carnegie Mellon University, which showed that .04% of the population could be re-identified by combining a “de-identified” data set with other public data.⁷⁵ In addition, Dr. Bradley Malin, Director of the Health Information Privacy Laboratory of Vanderbilt University, estimated that, using a “limited data set,” 68.4% of the population was re-identifiable.⁷⁶ Thus, it appears that the risk of re-identification of a “limited data set” is exponentially greater than the risk of re-identification of “de-identified” data.

Based on the comments received, the Commission affirms that “de-identified” data will not be deemed to be “PHR identifiable health information.” Given the small risk that such data will be re-identified by unauthorized third parties, the Commission

⁷³ SIIA at 9-10.

⁷⁴ *See, e.g.*, iGuard at 2; Quintiles at 2-3.

⁷⁵ CDT/Markle at 7; Columbia University at n. 6; World Privacy Forum at 8.

⁷⁶ Health Information Privacy Laboratory at Vanderbilt University at 1.

believes that the data would be more vulnerable if entities were required to re-identify these consumers solely to provide breach notification. Thus, de-identified data under HHS rules will not constitute “PHR identifiable health information,” and therefore, if such data is breached, no notification needs to be provided. On the other hand, the Commission declines to adopt a blanket statement that “limited data sets” are not “PHR identifiable health information” because the risk of re-identification is too high. The Commission similarly declines to state that “redacted, truncated, obfuscated, or otherwise pseudonymized data” does not constitute “PHR identifiable health information” because the risk of re-identification will depend on the context.

Even if a particular data set is not “de-identified,” however, entities still may be able to show, in specific instances, that there is no reasonable basis to identify individuals whose data has been breached, and thus, no need to send breach notices. For example, consider a website that helps consumers manage their medications. The website collects only email addresses, city, and medication information from consumers, but it keeps email addresses secured in accordance with HHS standards⁷⁷ and on a separate server. It experiences a breach of the server containing the city and medication information (but no email addresses). A hacker obtains medication information associated with ten anonymous individuals, who live in New York City. In this situation, the website could show that, even though a city is revealed, thus preventing the data from being categorized

⁷⁷ As noted below, the Recovery Act requires notification only if “unsecured” data has been breached, with the term “unsecured” to be defined by HHS. HHS issued guidance on the term “unsecured” on April 17, 2009. *See* 74 FR 19,006. The above example assumes the email addresses are secured in accordance with such guidance.

as “de-identified,” there is no reasonable basis for identifying the individuals, and no breach notification needs to be provided.

(f) PHR related entity

Proposed paragraph (f) defined the term “PHR related entity” as an 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 PHRs; or (3) “accesses information in a personal health record or sends information to a personal health record.”⁷⁸ The definition did not include HIPAA-covered entities or other entities acting as business associates of HIPAA-covered entities. The Commission adopts this definition without modification.

Several commenters raised questions about the first two categories. In particular, these commenters raised the question of whether the phrase “offers products or services through” a PHR website includes advertisers.⁷⁹ In its NPRM, the Commission had stated that PHR related entities would 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.” The Commission affirms that such entities are PHR related entities, but notes that they are only subject to the rule’s breach notification requirements if they experience a breach of “unsecured

⁷⁸ An entity that “accesses information in a personal health record or sends information to a personal health record” includes online applications through which individuals connect their blood pressure cuffs, blood glucose monitors, or other devices so that they can track the results through their PHRs. It also includes online medication or weight tracking programs that pull information from PHRs.

⁷⁹ See, e.g., SIIA at 10; World Privacy Forum at 5.

PHR identifiable health information” in a “personal health record.”⁸⁰ Thus, if they do not collect unsecured PHR identifiable health information at the website offering PHRs, they will not be subject to the rule’s breach notification requirements.⁸¹

One commenter stated that search engines appearing on PHR websites should be considered PHR related entities. This commenter noted that including such search engines within the rule’s scope is important because consumers may search for particular health conditions, and many search engines track individually identifiable information, such as the contents of previous searches, IP addresses, and cookies.⁸² In response, the Commission notes that search engines are PHR related entities if they appear on PHR websites, and are subject to the rule’s breach notification requirements if they collect unsecured PHR identifiable information at those websites.⁸³

⁸⁰ *See* Recovery Act, 13407(f)(1).

⁸¹ A consumer who clicks on an advertisement on the PHR website may be taken to the advertiser’s own site, where the advertiser may collect the consumer’s data. To avoid consumer confusion, and potentially deception, the advertiser should provide clear and conspicuous notice that the consumer is leaving the PHR website and that the advertiser’s privacy policy will now govern the collection of the consumer’s data.

⁸² World Privacy Forum at 4. For further discussion of privacy issues raised in this context, *see* FTC Staff Report, “Self-Regulatory Principles for Online Behavioral Advertising,” Feb. 2009, <http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

⁸³ Several commenters asked the Commission to clarify that an individual, such as a family member that accesses information in a relative’s PHR, is not a PHR related entity. *See, e.g.*, CDT/Markle at 6; UHG at 5. The Commission agrees that a family member who accesses information in a consumer’s PHR with the consumer’s authorization is not a PHR related entity.

(g) State

New paragraph (g) defines the term “State” as “any of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa and the Northern Mariana Islands.” This paragraph is identical to section 13400(15) of the Recovery Act and was added for reasons explained below, in the discussion of notice to the media.

(h) Third party service provider

Paragraph (g) of the proposed rule defined 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.” The Commission retains the definition of “third party service provider” without modification in the final rule and re-designates this paragraph as paragraph (h). Third party service providers include, for example, entities that provide billing, debt collection, or data storage services to vendors of personal health records or PHR related entities.

(i) Unsecured

Paragraph (h) of the proposed rule defined 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.” It further provided that, if such guidance is not issued by the date specified in such section, 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.” The Commission has removed the alternative definition from the final rule because HHS has already issued the required guidance under the Recovery Act.⁸⁴ The Commission also has re-designated this paragraph as paragraph (i).

(j) Vendor of personal health records

Paragraph (i) of the proposed rule defined 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.” The Commission retains this definition as proposed and re-designates it as paragraph (j).

Proposed section 318.3: Breach notification requirement

Paragraph 318.3(a) of the proposed rule required 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. The Commission retains this paragraph in the final rule without modification.

Paragraph 318.3(b) of the proposed rule required third party service providers of 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

⁸⁴ See *supra* note 77.

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) required that the third party service provider's notification include "the identification of each individual" whose information "has been, or is reasonably believed to have been acquired during such breach." The proposed paragraph also required third party service providers 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 Commission received several comments on paragraph 318.3(b), in response to which the Commission is making some changes to the final rule provision.

First, one commenter noted that a third party service provider may be unaware that it is dealing with a vendor of personal health records. For example, a cloud computing service provider⁸⁵ may offer computing power and storage without knowing whether customers use them to offer PHRs.⁸⁶ The Commission agrees with this comment and, accordingly, adds the following sentence to paragraph 318.3(b): "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."

Second, one commenter noted that some third party service providers may have multiple vendors of personal health records as clients.⁸⁷ If the third party service

⁸⁵ Cloud computing is the provision of Internet-based computer services. Cloud computing provides businesses and consumers with access to software, data storage, and infrastructure services that are hosted remotely.

⁸⁶ Microsoft at 3.

⁸⁷ SIIA at 9.

provider experiences a breach, it should not be required to identify every individual whose information was breached to each of its clients, regardless of whether the individual is a customer of the client. This could result in the third party service providers' sharing customer lists with competing vendors of PHRs, and could undermine the privacy of such customers. The Commission agrees. Thus, instead of requiring the third party service provider to identify each "individual" whose information was breached, the Commission's final rule requires the service provider to identify each "customer of the vendor of personal health records or PHR related entity" whose information was breached.⁸⁸

Third, several commenters supported the idea of having a specified official to whom the third party service provider would provide a breach notice.⁸⁹ However, some commenters stated that businesses should themselves agree upon these contact persons through their contractual arrangements.⁹⁰ The Commission agrees and amends the proposed rule to allow third party service providers to provide notice to "an official designated in a written contract by the vendor of personal health records or the PHR

⁸⁸ Some commenters raised the question of what would happen if a third party service provider did not have enough information to identify the individuals affected by the breach. *See, e.g.*, iGuard at 2; Quintiles at 2-3, SIIA at 8-9. In such case, the Commission expects that the third party service provider would provide the vendor or related entity with as much information as it has, after a thorough search of its records. Because the vendor or related entity has ultimate responsibility to provide individuals with notice, and likely possesses more comprehensive information regarding such individuals, the vendor or related entity must then take the data provided by the third party service provider and identify those individuals to whom notice must be provided.

⁸⁹ *See, e.g.*, AHIMA at 3, Statewide Parent Advocacy Network at 3.

⁹⁰ *See, e.g.*, NACDS at 2; SIIA at 9.

related entity to receive such notices, or, if such a designation is not made, to a senior official. . .” Because the purpose of this provision is to provide an efficient process for notifying consumers, the contact points designated by contract should be appropriate decisionmakers with sufficient responsibility and authority to oversee the process of notifying consumers. In designating an official, the parties also must consider that particular officials may move within the organization or leave altogether. Thus, it is important to establish a reliable mechanism for updating the designation when any such change occurs.

Fourth, the Commission received comments on the proposed rule’s requirement that the third party service provider obtain an acknowledgment of receipt of notice. Some commenters suggested that the third party service provider should merely retain evidence that notice was sent and that such evidence could be an email successfully sent or a certified mail receipt. These commenters expressed concern that requiring acknowledgment could delay sending of prompt notification to consumers.⁹¹ The Commission has not adopted this change. Even if the third party service provider retains evidence that someone signed for a package or opened an email, the communication may not have reached the intended recipient, particularly in a large, busy office. For example, in the case of a senior official, an assistant may open his or her email or a receptionist may sign for a package, but the senior official may never receive the communication. Moreover, the Commission does not believe that the requirement to acknowledge receipt will delay notice; the acknowledgment merely adds a check to ensure that the right

⁹¹ AHIP at 5-6; Molina Healthcare at 4; UHG at 5.

person will learn of the breach, and could be provided in the form of a simple return email.

Finally, paragraph 318.3(c) of the proposed rule provided 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 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.”

Some commenters expressed confusion about this standard and asked for clarification about when an employee’s knowledge should be imputed to an employer.⁹² The Commission interprets the Recovery Act as requiring that an employee’s knowledge be imputed to the employer. To clarify this point, the Commission modifies this provision to state that a breach “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

⁹² *See, e.g.*, Intuit at 3; Minnesota Department of Health at 4.

provider.” The Commission notes that a third party service provider may, in some cases, be an agent of a vendor of personal health records or PHR related entity; thus, when such a third party service provider discovers a breach, that knowledge would be imputed to the vendor or entity.⁹³

Section 318.4 Timeliness of Notification

Paragraph 318.4(a) of the proposed rule required that breach notifications to individuals and the media be “sent without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.” The Commission has modified this provision to clarify that the timeliness requirements apply to all notifications required to be provided under the rule, other than notification to the FTC.⁹⁴

⁹³ In addition, as noted in the NPRM, 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, the resulting failure to provide the appropriate breach notification 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.

⁹⁴ As noted in the NPRM, the standard for timely notification is “without unreasonable delay,” with the 60 day time 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 notification within 30 days, it would be unreasonable to wait until the 60th day to send the notice. Similarly, there may be circumstances where a vendor of personal health records discovers that its third party service provider has suffered a breach before the service provider notifies the vendor that the breach has occurred. Indeed, as noted in the text, if the third party service provider is an agent of a vendor of personal health records or PHR related entity, that service provider’s knowledge of the breach will be imputed to the vendor of personal health records or PHR related entity. In such circumstances, the vendor should begin taking steps to address the breach immediately, and should not wait

Thus, the provision now states that all notifications required “under §§ 318.3(a)(1), 318.3(b), and 318.5(b)” shall be sent without unreasonable delay.

Paragraphs 318.3(c) and 318.4(a) must be read together, with paragraph 318.3(c) establishing the time of “discovery” of the breach as the starting point for calculating the 60 day time period set forth in paragraph 318.4(a). The Commission received several comments with respect to the timing of notification. For example, one commenter asked whether an entity must establish that a breach involves “PHR identifiable health information” before the 60 day time period starts.⁹⁵ Another commenter requested guidance on the timing requirements if an entity determines that a breach affected a certain number of individuals and then later, perhaps close to the date it planned to send notices, realizes that the breach has affected more individuals.⁹⁶

In response to these comments, the Commission notes two points. First, an entity need not establish all the pre-requisites for triggering breach notification before the 60 day time period starts. Thus, for example, once an entity learns of possible unauthorized access to data, it cannot wait to conduct further investigation to determine whether unauthorized acquisition has occurred, whether PHR identifiable health information has been breached, or whether the information breached was unsecured. The purpose for the 60 day period is to give entities time to conduct such an investigation – the time period does not start when the investigation is complete.

until receiving notice from the service provider.

⁹⁵ Columbia University at 2-3.

⁹⁶ UHG at 6.

Second, the standard for determining timeliness is reasonableness. The breach has been “discovered” at the point when an entity reasonably should have known about it. The “reasonableness” standard applies equally with respect to the number of individuals affected. For example, if a breach affects 1,000 individuals, and the entity reasonably should have known that the breach affected all of these individuals on day 1, then the 60 day time period expires on calendar day 60. If, however, the entity undertook reasonable efforts to identify those affected by the breach and, despite such efforts, identified only 400 individuals on day 1 and the remaining 600 individuals on day 50, it is reasonable to take some additional time to send notices to the second round of 600 individuals. Because the entity already has information about the breach, however, it is probably not reasonable for the entity to wait an additional 60 days from the date it learned of these additional affected individuals to provide the notification.⁹⁷

Paragraph 318.4(b) of the proposed rule stated 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. The Commission adopts the proposed paragraph without change.

Paragraph 318.4(c) of the proposed rule provided that “[i]f 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” in the same manner as “45 CFR 164.528(a)(2). . .” The Commission adopts this proposed paragraph without modification.

⁹⁷ As described below, the entity must provide notice to the FTC within ten business days of learning that the breach affected 500 people.

Section 318.5 Methods of Notice

Section 318.5 of the proposed rule addressed 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.

Individual Notice

Proposed paragraph (a)(1) stated that an individual must be given notice by first-class mail or, if the individual provides express affirmative consent, by email. The paragraph also provided for notification to next of kin if the individual is deceased. Several commenters expressed concerns about the proposed paragraph.

First, although a few commenters supported requiring express affirmative consent for email notification,⁹⁸ the majority of commenters that addressed the issue opposed it.⁹⁹ Several of these commenters noted, as the Commission did in its NPRM, that email notice is particularly well-suited to the online relationship between consumers and vendors of personal health records and PHR related entities.¹⁰⁰ They also noted that entities may not wish to collect -- and consumers may not wish to provide -- mailing addresses.¹⁰¹ Indeed, several business commenters noted that they do not collect consumers' mail addresses, and that, if the Commission's proposed requirement became

⁹⁸ *See, e.g.*, IDEXperts at 3; AHIMA at 4.

⁹⁹ *See, e.g.*, ABC at 4; ACLI at 4-5; Association of Clinical Research Organizations ("ACRO") at 5; Dossia at 9; HealthITNow.org at 2; iGuard at 2-3; Microsoft at 2; Quintiles at 3; SIIA at 11.

¹⁰⁰ *See, e.g.*, ABC at 4; ACRO at 5; Quintiles at 3; SIIA at 11.

¹⁰¹ *See, e.g.*, HealthITNow.org at 2; Microsoft at 2.

final, they would need to request additional personal information from consumers that these consumers might not choose to share. These businesses also expressed uncertainty on how to proceed if existing consumers did not respond to such a request.¹⁰²

The Commission is persuaded that, because the relationships contemplated among vendors of personal health records, PHR related entities, and consumers take place entirely online, email notice is an appropriate default option. The Commission agrees with the commenters that stated that requiring express affirmative consent for email would result in entities' collecting additional personal information they otherwise would not collect, and that consumers may not want to provide.

However, the rule must still follow the Recovery Act, which requires that entities can only send notice by email "if specified as a preference by the individual." The Commission interprets this phrase as requiring entities to provide consumers with a meaningful choice to receive email notice. For a choice to be meaningful, the entity must provide clear and conspicuous notice to consumers that they have such a choice. Thus, entities may not merely state in their terms and conditions that they will send relevant notices by email unless an individual objects.

Entities can, however, provide meaningful choice by sending their customers an email or posting an alert that appears when they access their account, which (1) informs them that they will receive breach notices by email, and (2) provides them with a reasonable opportunity to express a preference to receive such notices by first-class mail. The entity could provide such a "reasonable opportunity" by including a toll-free

¹⁰² *See, e.g.*, iGuard at 2-3; Microsoft at 3.

number, a return email address, or a link in the notice or alert allowing consumers to opt out of email notification and select first-class mail instead. The Commission would not consider requiring the consumer to write a letter as offering a reasonable opportunity to express such a preference. Entities choosing this approach also must inform consumers that, if they do not affirmatively make a choice, they will receive breach notices by email.

Accordingly, the Commission has adopted the following language into final paragraph 318.5(a)(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.”

Second, the Commission requested information on how to address the problem posed by some email notifications being screened by consumers’ spam filters. One commenter suggested that the Commission require entities to verify receipt of breach notifications.¹⁰³ The Commission declines to adopt this suggestion because entities may be unable to verify receipt, particularly if verification requires some action by the consumer (such as a return email confirming receipt). This could leave entities no choice but to provide alternative notice, which could in turn result in consumers’ receiving multiple notices for the same breach. Another commenter suggested that vendors of personal health records and PHR related entities should (1) notify individuals that breach notices may be blocked by spam filters and (2) provide them with guidance on how to set

¹⁰³ EPIC at 10.

spam filter preferences to ensure they receive these notices.¹⁰⁴ The Commission agrees that entities who send breach notices by email should provide guidance to consumers regarding how properly to set up spam filters so that they will receive such notices.

Third, some commenters expressed concern about the requirement that breach notices be sent to an individual's next of kin if the individual is deceased.¹⁰⁵ One such commenter pointed out that consumers may not want their next of kin to know about their PHRs.¹⁰⁶ The Commission agrees, and accordingly modifies paragraph 318.5(a)(1) to read as follows: "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."

Finally, the Commission received comments suggesting other forms of direct notice to individuals. One commenter suggested that breach notices be available in formats such as large font, Braille and audiotape.¹⁰⁷ Another commenter advocated the use of text messaging and social networking to notify individuals.¹⁰⁸ Some commenters suggested that entities provide consumers with non-avoidable notices directly into their

¹⁰⁴ Identity Theft 911 at 3.

¹⁰⁵ *See, e.g.*, ACLI at 5; Minnesota Department of Health at 5.

¹⁰⁶ Minnesota Department of Health at 5.

¹⁰⁷ American Association of People with Disabilities at 2.

¹⁰⁸ EPIC at 9.

accounts.¹⁰⁹ Section 13402(e)(1) of the Recovery Act requires that notification be provided via “written notification by first-class mail” or “electronic mail.” Because the rule must follow this mandate, none of the suggested alternative methods can replace mail or email. The Commission notes, however, that the rule does not preclude any of these forms of notice, and supports their use in appropriate circumstances, in addition to the forms of notice prescribed in the rule.

The Commission has changed the remainder of proposed paragraph (a). It has combined proposed paragraphs (a)(3) and (a)(4), addressing substitute notice to individuals, into a new paragraph (a)(2), to immediately follow the rule provision addressing direct notice to individuals. Proposed paragraph (a)(3) stated that if, after making reasonable efforts to contact an individual through his or her preferred method of communication, the vendor 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. Proposed paragraph (a)(4) stated that if ten or more individuals cannot be reached, the vendor of personal health records or PHR related entity must provide substitute notice through its website home page or through the media.

These proposed rule paragraphs prescribed a two step process for substitute notice: First, they required entities to provide a substitute form of actual notice (e.g., the

¹⁰⁹ *See, e.g.*, Healthcare Information and Management Systems Society at 2; World Privacy Forum at 6.

individual's less preferred method of actual notice, telephone, or other means) for all individuals for whom there was insufficient contact information. Second, if, after making this attempt to provide substitute actual notice, "ten or more individuals [could] not be reached," the entity was required to provide notice through the home page of its website or through the media.

The final paragraph (a)(2) combines these paragraphs into one paragraph that prescribes substitute notice through media or web posting, if "after making reasonable efforts to contact all individuals. . .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 Commission has made this change for several reasons.

First, the proposed rule paragraphs had required that all entities attempt to provide substitute notice through the individual's less-preferred method of communication, a telephone call, or other appropriate means before providing substitute notice through media or web posting. Some commenters expressed concern about references to "preferred" and "less preferred" methods, suggesting that such language would require entities to track lists of consumers' preferences with respect to notice.¹¹⁰ Other commenters stated that entities may collect only one form of contact information, usually email.¹¹¹ The Commission agrees that the rule should not refer to "preferred" or "less-preferred" or other methods of direct notice, particularly given that vendors of personal health records and PHR related entities may only collect email addresses and no other

¹¹⁰ *See, e.g.*, ACLI at 5; NAMIC at 5.

¹¹¹ *See, e.g.*, iGuard at 2-3; Quintiles at 3.

contact information from consumers. Because the Commission does not want to encourage entities to collect more contact information than is necessary, the rule no longer requires entities to contact individuals through another form of direct notice in every case.

Second, the proposed rule had required substitute notice “if ten or more individuals cannot be reached.” One commenter expressed concerns that the “cannot be reached” language requires confirmation of receipt.¹¹² The new paragraph makes clear that no such confirmation is required; rather, the rule requires “reasonable efforts to contact all individuals.” For example, in the case of incomplete contact information, reasonable efforts would include searching internal records and, if needed, undertaking additional reasonable efforts to obtain complete and accurate contact information from other sources. In addition, the standard, while not requiring confirmation, requires an entity to take reasonable steps to contact consumers by other practical, available means when it knows that the initial contact method has been unsuccessful. If the entity knows that an individual has not received such notice (e.g., an email is returned as undeliverable), reasonable efforts would include (1) if the entity has the individual’s mailing address, sending written notice to that address; or (2) if the entity has the individual’s telephone number, calling the individual to obtain updated contact information for purposes of providing direct notice.¹¹³

¹¹² UHG at 6-7.

¹¹³ *Cf. Jones v. Flowers*, 547 U.S. 220 (2006) (stating that the government’s obligation to provide direct notice of foreclosure to taxpayer was not satisfied by sending a letter by certified mail, having it returned as unclaimed, and then posting the notice in the newspaper; another form of direct notice was required where possible and practicable).

Turning to the requirements for substitute notice through home page or media notice, the proposed rule allowed for (1) a conspicuous notice on the home page of the entity's website for a period of 6 months; or (2) notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach reside. Such home page or media notice was required to include a toll-free phone number where an individual could learn whether the individual's information was included in the breach. The Commission received several comments on this paragraph.

First, one commenter expressed concern about the rule's requiring a toll-free number for individuals to determine whether their information was breached. This commenter noted the difficulties associated with authenticating callers over the telephone and recommended alternate approaches to letting consumers know if their information was breached.¹¹⁴ Because the Recovery Act mandates the provision of a toll-free telephone number, the Commission declines to remove this requirement from the final rule. The Commission does, however, share the concerns expressed by commenters about how entities would authenticate callers to the toll-free line for the purposes of providing information specific to the caller. In particular, entities should not ask consumers who call the toll-free line for Social Security numbers or financial account numbers because requesting such information may raise concerns about "phishing," or may even increase the risks of "phishing."¹¹⁵ Entities also may choose to provide only general information to consumers who call the toll-free line and inform those consumers that they will send more

¹¹⁴ Microsoft at 5.

¹¹⁵ For example, if such requests for information become customary and accepted, consumers may not be sufficiently cautious in responding to them.

specific information to the consumer's PHR or related account, or the email address they provided to set up their account.¹¹⁶

Second, with respect to posting on the home page,¹¹⁷ most commenters that addressed the issue stated that the six month required posting period in the proposed rule was too long. These commenters generally suggested a shorter posting period, anywhere from 30 to 90 days.¹¹⁸ Several of these commenters stated that a six month posting period could confuse or unduly alarm consumers every time they accessed the entity's web page.¹¹⁹ Other commenters suggested that a requirement for a six month posting placed a burden on businesses that was not commensurate with the potential advantages to individuals.¹²⁰

¹¹⁶ The final rule clarifies that the toll-free number must remain active for at least 90 days.

¹¹⁷ As stated in the NPRM, 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 involve an online relationship, web posting would be a particularly well-suited method of substitute notice to individuals.

¹¹⁸ *See, e.g.*, ACLI at 5; ACRO at 5; Dossia at 10; iGuard at 3; NACDS at 3; NAMIC at 6; Minnesota Department of Health at 5; Ohio State University Medical Center at 2; Quintiles at 3-4; Sonnenschein at 3.

¹¹⁹ *See, e.g.*, NACDS at 3; Ohio State University Medical Center at 2.

¹²⁰ *See, e.g.*, NAMIC at 6; Sonnenschein at 3.

After reviewing the comments, the Commission has decided to change the time period for posting of the website notice in the final rule to ninety days.¹²¹ The Commission believes that this time period is long enough to provide an effective form of substitute notice, while also avoiding unnecessary consumer confusion and alarm.¹²²

Third, some commenters urged the Commission to interpret the requirement to provide media notice “in major print or broadcast media” to allow such notice through new technology, such as notice in major Internet media and news outlets.¹²³ One commenter argued that the Recovery Act requirement to provide notice in “print or broadcast” media should not be limited to print, radio, and television outlets because the term “broadcast” means making information known over a wide area.¹²⁴ Although the Commission recognizes the importance of the Internet as a medium, the Commission believes that the term “broadcast media” in the Recovery Act is limited to traditional radio

¹²¹ This 90 day period for web posting begins after entities have satisfied their notice obligation specified in paragraph (a)(1).

¹²² As stated in the NPRM, 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.

One commenter recommended that the Commission incorporate this guidance into the text of the final rule. AHIMA at 4. Given that new technologies may provide new ways to satisfy a requirement of “conspicuousness” and render old ways potentially obsolete, the Commission declines to incorporate its specific guidance regarding conspicuousness into the final text of paragraph 318.5(a)(4).

¹²³ CDT/Markle at 12-13; EPIC at 9-10.

¹²⁴ CDT/Markle at 13.

and television news outlets. Indeed, if the Commission were to construe the term more broadly to include making information known over a wide area, the Recovery Act's reference to "print" media would be superfluous. Accordingly the Commission does not read the phrase "print or broadcast media" to include Internet media and news outlets.¹²⁵ However, the Commission encourages entities to provide notice through major Internet media, in addition to providing notice through print or broadcast media, if such additional notice would increase the likelihood of reaching affected consumers.

Fourth, some commenters asked how they could satisfy the requirement to provide media notice "in geographic areas where the individuals affected by the breach likely reside" if they do not collect address information.¹²⁶ The Commission believes that, if entities do know where individuals affected by the breach reside, they should target substitute media notice to those areas. If they do not know where individuals reside, they should notify media on a nationwide basis.¹²⁷ The Commission does not interpret the

¹²⁵ As stated in the NPRM, 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, if known, 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 or 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" under the rule if it is clear and conspicuous. Thus, the notices should be stated in plain language, be prominent, and run multiple times.

¹²⁶ AHIP at 5; Molina Healthcare at 3.

¹²⁷ The Commission notes that entities are never *required* to provide substitute notice to individuals through the media under this provision; they also have the option of

reference to where individuals “likely reside” as a requirement to collect address information from customers.¹²⁸

Finally, proposed paragraph (a)(2) allowed a vendor of personal health records or PHR related entity to provide notice by telephone or other appropriate means, in addition to notice by first-class mail or email, if there is possible imminent misuse of unsecured PHR identifiable health information. The Commission adopts this language without change and has redesignated it as paragraph (a)(3) in the final rule.

Notice to Media if the Breach Affects 500 or More Individuals

Proposed paragraph 318.5(b) required 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 such State or jurisdiction.” This media notice differs from the substitute media notice described in paragraph 318.5(a)(4) in that it is directed “to” the media and is intended to supplement, but not substitute for, individual notice. The Commission has not made any substantive changes to this paragraph,¹²⁹ but clarifies two issues in response to comments received.

First, some commenters expressed confusion about the meaning of the phrase “State or jurisdiction” in this paragraph.¹³⁰ To clarify the phrase, and to track section

providing notice through a home page posting.

¹²⁸ The proposed rule had required that media notice be “reasonably calculated to reach the individuals affected by the breach.” The Commission has moved this language to clarify that any form of substitute notice, including media notice and web page posting, must be “reasonably calculated to reach the individuals affected by the breach.”

¹²⁹ However, the Commission has deleted the second sentence of the rule setting forth the content requirements for such notice as redundant.

¹³⁰ *See, e.g.,* Molina Healthcare at 4; NAMIC at 6.

13400(15) of the Recovery Act, the Commission has added a definition of the word “State” to include “any of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.” In addition, the Commission interprets the term “jurisdiction” to mean a geographic area smaller than a state, such as a county, city, or town. This interpretation ensures that, if a breach affects such a specific area, the media notice will be targeted to that area. Accordingly, notice to media is required if a breach affects more than 500 individuals in a particular state, the District of Columbia, a territory or possession of the United States, or a smaller geographic subdivision.¹³¹ If no single state has more than 500 people affected, notice to media is not required.

Second, as with substitute media notice, some commenters urged the Commission to interpret this paragraph to allow notification to prominent Internet-based media outlets.¹³² Unlike the requirement to provide substitute notice in “print or broadcast” media described above, the Recovery Act does not limit this notice to particular types of media. Thus, an entity can satisfy the requirement to notify “prominent media outlets” under this paragraph by disseminating press releases to a number of media outlets, including Internet media in appropriate circumstances, where most of the residents of the

¹³¹ If an entity experiences a breach that affects more than 500 people in a city such as New York City, as well as more than 500 people elsewhere in the state, the entity has an obligation to provide notice to prominent media outlets both in New York City and New York state.

¹³² CDT/Markle at 12-13; EPIC at 9-10.

relevant state or jurisdiction get their news. This will be a fact-specific inquiry that will depend upon what media outlets are “prominent” in the relevant jurisdiction.¹³³

Notice to the Commission

Proposed paragraph 318.5(c) required vendors of personal health records and PHR related entities to notify 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, the proposed paragraph allowed vendors of personal health records and PHR related entities, in lieu of immediate notice, to maintain a breach log and submit this log annually to the Commission. The proposed rule stated that the “annual log” would be due one year from the date of the entity’s first breach. As described below, the Commission received a number of comments on this proposed paragraph and has made some modifications to the final rule in response.

First, the Commission received many comments objecting to the proposed paragraph’s requirement that entities provide notice to the Commission no later than five business days after discovery of a breach affecting 500 or more individuals. These commenters argued that five business days did not allow sufficient time to conduct an investigation and might lead entities to report information to the Commission that later

¹³³ For example, an entity could satisfy this requirement by sending a press release to the relevant division or department (e.g., health, technology, or business) of a number of prominent print publications, cable news shows, radio stations, and Internet news media outlets. The number of outlets and combination of media will vary, depending on the circumstances of the breach.

turns out to be incorrect.¹³⁴ The Commission agrees that a five day notice requirement could create burdens for companies without corresponding benefits, particularly if the shorter notice period results in false reporting of breaches. Thus, the Commission has decided to expand the time period for notice to the FTC from five business days to ten business days. The Commission believes that this time period still satisfies the Recovery Act's mandate that notice to the Commission be "immediate," while allowing entities additional time to investigate the circumstances surrounding the breach before notifying the FTC.¹³⁵

Second, several commenters recommended that the annual log to the Commission for breaches involving fewer than 500 individuals be submitted each calendar year, instead of one year from the date of the entity's first breach.¹³⁶ As a few commenters stated, calendar year reporting would allow the Commission to aggregate the number of breaches reported by all entities in a given year.¹³⁷ It also would simplify the process of reporting breaches by allowing organizations to prepare their logs systematically, with a fixed deadline.¹³⁸ The Commission agrees with these comments and has modified the

¹³⁴ *See, e.g.*, AHIMA at 4-5; AHIP at 6; Dossia at 9; Microsoft at 4-5; Molina at 5; NACDS at 3; Sonnenschein at 2-3; UHG at 7-8; WebMD at 5.

¹³⁵ The Commission recognizes that entities may need more than ten business days to fully investigate the breach, and that the initial information provided to it in that time period may not be complete.

¹³⁶ *See, e.g.*, ACRO at 5; AHIP at 6-7; iGuard at 3-4; Minnesota Department of Health at 5; Molina Healthcare at 5; NAMIC at 7; Quintiles at 4; UHG at 8-9.

¹³⁷ *See, e.g.*, ACRO at 5; iGuard at 3-4; Quintiles at 4.

¹³⁸ *See, e.g.*, Minnesota Department of Health at 5; NAMIC at 7; UHG at 8-9.

final rule to allow for calendar year reporting as follows: “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 within 60 calendar days following the end of the calendar year, documenting breaches from the preceding calendar year.”¹³⁹

Third, a few commenters made suggestions on how the Commission should collect and organize the notices it receives. One commenter recommended that the Commission create a comprehensive repository of information concerning data breaches.¹⁴⁰ Raising security concerns, one industry commenter recommended that the Commission designate a point person or office to receive notices by registered or express mail, and treat all such information as business confidential, not subject to release under the Freedom of Information Act (“FOIA”).¹⁴¹ Other commenters encouraged the FTC to require entities not to report individually identifiable information.¹⁴²

Consistent with these comments, the Commission has developed the attached form, which it will post at www.ftc.gov/healthbreach, for vendors of personal health records or PHR related entities subject to the rule to complete for purposes of notifying the FTC when they discover a breach. The form’s instructions require entities to print and

¹³⁹ No annual log needs to be provided for years in which no breaches occur. In addition, for calendar year 2009, the regulated entity is only required to submit information to the FTC for breaches occurring after the effective date of this regulation.

¹⁴⁰ EPIC at 10.

¹⁴¹ SIIA at 12.

¹⁴² *See, e.g.*, AHIP at 7; Molina Healthcare at 5.

send the form to a designated FTC official by courier or overnight mail. Due to security concerns associated with email transmission, the Commission will not accept emailed forms at this time. Also, the form instructs entities not to include consumers' personally identifiable information in their notice to the FTC.¹⁴³

Until an entity sends a breach notice to consumers, the FTC will not routinely make public any information the entity provides to it on the breach notification form.¹⁴⁴ Once an entity sends a breach notice to consumers, however, the FTC will input the information it receives from the entity into a database that it will update periodically and make available to the public.

Section 318.6 Content of Notice

Proposed section 318.6 required that the breach notice to individuals include 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; 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;¹⁴⁵ a brief description of what the

¹⁴³ Entities should begin using this form to provide notice to the Commission beginning on the effective date of this rule. However, pursuant to regulations of the Office of Management and Budget ("OMB"), the Commission will issue a separate Federal Register notice seeking comments on the form; based on comments received, the Commission may modify the form in the future.

¹⁴⁴ In response to a request under the Freedom of Information Act, however, the FTC may be required to disclose information provided on the form in response to a request from the public, unless the information contains confidential business information or other information exempt from public disclosure under that Act. 5 U.S.C. 552.

¹⁴⁵ As stated in the NPRM, the steps individuals should take to protect themselves from potential harm will differ depending on the circumstances of the breach

vendor of personal health records or PHR related entity involved is doing to investigate the breach, to mitigate any harm, and to protect against any further breaches; and contact procedures for individuals to ask questions or learn additional information.¹⁴⁶ In response to comments received, the Commission has made three changes to this section.

and the type of PHR identifiable information involved. For example, if health insurance account information is compromised, 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. 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.

One commenter recommended that the Commission incorporate this guidance into the text of the final rule. AHIMA at 5. Because these steps will differ depending on the circumstances of the breach and in light of the variety of factual situations that may be involved, the Commission has not incorporated its specific guidance into the final text of section 318.6.

¹⁴⁶ In its NPRM, the Commission stated also that the breach notice should not include any requests for personal or financial information, which could raise concerns about phishing.

First, it has replaced references to mitigating “losses” from a breach with the term “harm,” to more precisely reflect that injury from a health-related breach is not restricted to economic loss.

Second, some commenters noted that the requirement that the notice contain “a brief description of how the breach occurred” might create unnecessary security risks by inadvertently providing a roadmap for future breaches. These commenters urged the Commission to track the language of the Recovery Act which requires “a brief description of what happened.”¹⁴⁷ The Commission is persuaded by these comments and modifies the language of 318.6(a) so that it reads as follows: “a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.”

Finally, to ensure that notice be simple and non-technical so that individuals easily can understand the information being conveyed, the Commission has added language to this section mandating that the notice “be written in plain language.” In order to satisfy this requirement, entities should use clear language and syntax in their notices, and not include any extraneous material that might diminish the message they are trying to convey. In addition, entities should not include content beyond that required by law (including state law if the notice is designed to comply with both federal and state requirements), if such additional content could cause consumer confusion.

Sections 318.7, 318.8, 318.9: Enforcement, Effective date, and Sunset

The Commission retains sections 318.7, 318.8, and 318.9 as proposed. With respect to the effective date of 30 days from publication of the final rule, however, at least

¹⁴⁷ See, e.g., CDT/Markle at 11; SIIA at 13.

one commenter expressed concern that such an effective date does not allow enough time to implement the processes and procedures necessary to comply with the FTC's rule.¹⁴⁸ Although the Commission does not have discretion to change the effective date of the rule because the Recovery Act establishes the effective date, which is mandated by the Recovery Act, it recognizes that entities may need to develop new procedures to comply with it. Therefore, the Commission will use its enforcement discretion to refrain from bringing an enforcement action for failure to provide the required notifications for breaches that are discovered before [insert date 180 days after date of publication in the FEDERAL REGISTER]. During this initial time period – after this rule has taken effect but before an entity is subject to an enforcement action – the Commission expects regulated entities to come into full compliance with the final rule.

IV. Paperwork Reduction Act

In conjunction with the NPRM, the FTC submitted the proposed rule and a Supporting Statement to the Office of Management and Budget (“OMB”) for review under the Paperwork Reduction Act (“PRA”). The breach notification requirements contained in the proposed rule constituted “collections of information,” which triggered the requirements of the PRA. In response, OMB filed a comment in accordance with 5 C.F.R § 1320.11(c). The comment indicated that OMB was withholding approval pending (1) the FTC's examination of the public comments in response to the NPRM, and (2) inclusion of a description in the preamble to the final rule of how it has maximized the practical utility of the collection of information and minimized the burden. In this section,

¹⁴⁸ Intuit at 3.

the Commission (1) describes how it has maximized the practical utility of the final rule, and (2) sets forth a revised PRA analysis, taking into account both changes made to the proposed rule and comments received in response to its initial PRA analysis.

A. Practical Utility

According to OMB regulations, practical utility means the usefulness of information to or for an agency.¹⁴⁹ In determining whether information will have “practical utility,” OMB will consider “whether the agency demonstrates actual timely use for the information either to carry out its functions or make it available to third-parties or the public, either directly or by means of a third-party or public posting, notification, labeling, or similar disclosure requirement, for the use of persons who have an interest in entities or transactions over which the agency has jurisdiction.”¹⁵⁰

The Commission has maximized the practical utility of the breach notification requirements contained in the final rule, consistent with the requirements of the Recovery Act. Under the final rule, consumers whose information has been affected by a breach of security will receive notice of it “without unreasonable delay and in no case later than 60 calendar days” after discovery of the breach.¹⁵¹ Among other information, the notices must provide consumers with steps they can take to protect themselves from harm. Moreover, the breach notice requirements will encourage entities to safeguard the information of their customers, thereby potentially reducing the incidence of harm.

¹⁴⁹ 5 CFR 1320.3(l).

¹⁵⁰ *Id.*

¹⁵¹ 16 CFR 318.4(a).

As provided by the Recovery Act, the final rule also requires entities to notify the Commission in the event of a security breach. The Commission has developed a form, which it will post at www.ftc.gov/healthbreach, for entities subject to the rule to complete for this purpose. The form requests minimal information, mostly in the form of replies to check boxes; thus, entities will not require extensive time to complete it. At the same time, the form will provide a significant source of enforcement leads for the Commission. The Commission also will input the information it receives from entities into a database that it will update periodically and make available to the public. The publicly-available database will help businesses, the public, and policymakers. It will provide businesses with information about potential sources of data breaches, which will be particularly helpful to those setting up data security procedures. It will provide the public with information about the extent of data breaches. And it will help policymakers in developing breach notification requirements in non-health-related areas.

Thus, the final rule will have significant practical utility.

B. Explanation of Burden Estimates Under the Final Rule

The PRA burden of the final rule's 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.

In its initial PRA analysis, staff estimated that approximately 200 vendors of personal health records and 500 PHR related entities will be covered by the Commission's final rule. Thus, it estimated that a total of 700 entities will be required to notify consumers and the Commission in the event that they discover a breach. It also estimated

that approximately 200 third party service providers will also 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, staff estimated that a total of approximately 900 entities will be subject to the final rule's breach notification requirements. The staff retains these estimates without modification.

Staff estimated 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 final 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 2007.¹⁵² Dividing 50 breaches by the estimated number of firms that would be subject to a breach (4,187)¹⁵³ yields an estimated breach

¹⁵² 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 other data staff used to calculate the incidence of breaches.

¹⁵³ 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

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. The staff retains this estimate without modification.

To determine the annual PRA burden, staff 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 estimated that covered firms will require per breach, on average, 100 hours of employee labor at a cost of \$4,652,¹⁵⁴ and the services of a forensic expert at an estimated cost of \$2,930.¹⁵⁵ Thus, the cost estimate for each breach was \$7,582. This

only one percent of these firms had security vulnerabilities that would render them breach targets, thus yielding the total of 4,187.

¹⁵⁴ 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, 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.

¹⁵⁵ 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.

estimate did 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 was estimated to be \$83,402 (11 breaches x \$7,582 each).

The Commission received one comment suggesting that the staff's estimate of 100 hours of employee labor to determine what information has been breached, identify the affected customers, prepare the breach notice, and make the required notice to the Commission might be too low. This commenter noted that the analysis did not take into account the burden caused by compliance with potentially duplicative and conflicting state requirements.¹⁵⁶

Staff has not altered its PRA burden analysis based on this comment. First, as discussed above, the final rule preempts any conflicting state law. Second, several of the potential costs or time burdens raised by the commenter, including those incurred to comply with preexisting, albeit duplicative state laws, or those associated with public relations and marketing, are not functions constituting a PRA "collection of information."¹⁵⁷ Finally, although the Commission recognizes that certain entities may

¹⁵⁶ SIIA at 14.

¹⁵⁷ The PRA burden analyzed here includes the time, effort and financial resources expended by covered entities to generate, maintain, or provide information to or for the Commission on account of the rule. *See* 5 CFR 1320.3(b)(1). "Collection of information means . . . requiring the disclosure to an agency, third parties or the public of information by or for an agency by means of identical questions posed to, or identical reporting, recordkeeping, or disclosure requirements imposed on, ten or more persons . . ." 5 CFR 1320.3(c).

spend more than 100 hours regarding the above-noted tasks, staff's hours estimate is an average of the burden that would be incurred across small and large businesses experiencing various types of breaches.

The cost of breach notifications also 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.¹⁵⁸ Staff estimated 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 estimated that an average of 232,000 consumers per year will receive a breach notification. Staff retains this estimate without modification.

Given the online relationship between consumers and vendors of personal health records and PHR related entities, staff stated that most notifications will be made by email and the cost of such notifications will be de minimis.¹⁵⁹

In some cases, however, staff noted that 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 estimated that the cost of notifying an

¹⁵⁸ 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.

¹⁵⁹ See Federal Trade Commission, National Do Not Email Registry, A Report to Congress, June 2004, n.93, available at www.ftc.gov/reports/dneregistry/report.pdf.

individual by postal mail will be approximately \$2.30 per letter.¹⁶⁰ 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. Staff retains this estimate.

In addition, staff recognized that 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 estimated 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.¹⁶¹ Applied to the 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. Staff retains this estimate without modification.

Finally, staff assessed that the cost of a toll-free number will depend on the cost associated with T1 lines¹⁶² sufficient to handle the projected call volume, the cost of

¹⁶⁰ 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.

¹⁶¹ Ponemon Institute, 2006 Annual Study: Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions, Table 2.

¹⁶² A T1 line is a specific type of telephone line that can carry more data than traditional telephone lines.

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. In the NPRM, staff estimated the cost of a toll-free line for a six-month period, because the proposed rule provided that entities choosing to post a message on their homepage do so for a period of six months. Because the Commission has changed this homepage posting requirement to ninety days in response to comments, staff now estimates the cost of a toll-free line for a ninety-day 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 \$9,000.¹⁶³ Staff further estimates that the cost of obtaining a dedicated toll-free line and queue messaging will be \$3,017,¹⁶⁴ 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 \$27,468.¹⁶⁵ Affected entities will need to offer the toll-free number for an additional two months, during which time staff projects that entities will each cumulatively receive an additional 3,000 calls per breach,¹⁶⁶ yielding an estimated total processing cost of \$43,946 (\$27,468 + \$16,478). In

¹⁶³ According to industry research, the cost of a single T1 line is \$1,500 per month.

¹⁶⁴ 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.

¹⁶⁵ 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. This totals \$27,468.

¹⁶⁶ Staff anticipates that the greatest influx of calls will be in the first month, and that the volume of calls will be less for the next two months. The breakdown of labor

addition, according to industry research, the telecommunication charges associated with the toll-free line will be approximately \$2,000.¹⁶⁷ Adding these costs together, staff estimates that the cost per breach for the toll-free line will be \$57,963. Based on the above rate of 11 breaches per year, the annual cost burden for affected entities will be \$637,593 (11 x \$57,963).

In sum, the estimated annual cost burden associated with the breach notification requirements of the final rule is \$795,235: \$83,402 (costs associated with investigating breaches, drafting notifications of breaches, and notifying the Commission) + \$74,240 (costs associated with notifying consumers) + \$637,593 (costs associated with establishing toll-free numbers). Staff notes that this estimate likely overstates the costs imposed by the final 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.

V. Final Regulatory Flexibility Analysis

The Regulatory Flexibility Act ("RFA"), 5 U.S.C. 604(a), requires an agency either to provide a Final Regulatory Flexibility Analysis ("FRFA") with the final rule, or

hours and costs for this two-month period is as follows: 400 hours of telephone operator time (8 minutes per call x 3,000 calls) at \$14.87 per hour and 750 hours of information processor time (15 minutes per call x 3,000 calls) at \$14.04 per hour. This totals \$16,478.

¹⁶⁷ Staff estimates a cost per call of 25¢ (5¢ per minute/per call x 5 minutes per call). Assuming 8,000 calls for each breach, the total estimated telecommunications charges are \$2,000.

certify that the final rule will not have a significant economic impact on a substantial number of small entities. The Commission does not expect that this final rule will 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 final 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.¹⁶⁸ 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 email. Based on available information, therefore, the Commission certifies that the final rule will not have significant economic impact on a substantial number of small entities.

Nonetheless, to ensure that no such impact, if any, has been overlooked, the Commission has conducted the following final regulatory flexibility analysis, as summarized below.

A. Need for and Objectives of the Rule

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 17, 2009. The Commission is issuing this rule to implement the Recovery Act's requirement that certain entities that handle health information provide notice to individuals whose individually identifiable health information has been breached.

¹⁶⁸ See, e.g., Ark. Code 4-110-103(5); Ca. Civil Code 1798.81.5; Md. Code, Com. Law § 14-3501(D)(1).

B. Significant Issues Raised by Public Comment, Summary of the Agency's Assessment of These Issues, and Changes, if any, Made in Response to Such Comments

The Commission did not receive any substantive comments on its proposed Regulatory Flexibility Act analysis. Nonetheless, the Commission provides an overview here of the significant comments it received that would affect the costs of complying with the rule for all entities, small and large, and its response.

First, several commenters stressed that FTC and HHS should work together to ensure that their respective breach notification rules are harmonized and that stakeholders know which rule applies to which entity.¹⁶⁹ These commenters recognized that some entities may be subject to both rules, and that it is therefore important for the rules to be similar.¹⁷⁰ The Commission agrees with these comments and has consulted with HHS to harmonize the two rules, within the constraints of the statutory language.

Second, commenters raised several concerns about the timing and method of breach notification that would affect businesses of all sizes. For example, commenters that addressed the issue generally opposed requiring an entity to secure a consumer's "express affirmative consent" before sending breach notices by email.¹⁷¹ For the requirement to provide substitute notice to individuals on the home page of an entity's website, many commenters opposed the six month required posting period and suggested

¹⁶⁹ *See supra* note 7.

¹⁷⁰ *See supra* note 8.

¹⁷¹ *See supra* note 99.

that a shorter period would be less burdensome for businesses and less confusing for consumers.¹⁷² Finally, many commenters objected to the proposed rule's requirement that entities provide notice to the Commission no later than five business days after discovery of a breach affecting more than 500 individuals.¹⁷³

As discussed in more detail above, in response to these concerns, the Commission made several changes to the rule, all of which will reduce the burden on entities of all sizes while also ensuring meaningful breach notification to consumers. Specifically, rather than require express affirmative consent for email notice, the final rule allows entities to have their customers opt out of receiving email notice. The final rule also reduces the home page posting period from six months to ninety days, and extends the time period for providing the Commission with notice of large breaches, from five to ten business days.

Finally, other commenters expressed concerns about particular statutory requirements governing breach notification that come directly from the Recovery Act (for example, whether media notice may be too burdensome).¹⁷⁴ Because these requirements come directly from the Recovery Act, the Commission cannot change its final rule in response to these comments. Nevertheless, as discussed above, the Commission will take these comments into account when providing input on the HHS report.

¹⁷² *See supra* note 118.

¹⁷³ *See supra* note 134.

¹⁷⁴ *See supra* notes 19-20.

C. Description and Estimate of the Number of Small Entities Subject to the Final Rule or Explanation Why No Estimate Is Available

The final rule will apply to vendors of personal health records, PHR related entities, and third party service providers. As discussed in the section on PRA above, FTC staff estimates that the rule will apply to approximately 900 entities. Staff continues to believe that the available data about the relatively new PHR industry is not sufficient for staff to estimate realistically the number of entities subject to the FTC's final rule that are small as defined by the Small Business Administration.¹⁷⁵

D. Description of the Projected Reporting, Disclosure and Other Compliance Requirements of the Rule, Including an Estimate of the Classes of Small Entities That Will be Subject to the Rule and the Type of Professional Skills That Will be Necessary to Comply

The Recovery Act and final rule impose certain reporting and disclosure requirements within the meaning of the PRA. The Commission is seeking clearance from 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 final 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 final rule also

¹⁷⁵ For a majority of the entities subject to the rule to be considered small businesses, they must have average annual receipts that are \$7 million or less. A list of the SBA's size standards for all industries can be found at http://www.sba.gov/idc/groups/public/documents/sba_homepage/serv_sstd_tablepdf.pdf (last visited July 24, 2009).

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.

As discussed in the section on PRA above, if a breach occurs, each entity covered by the final 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 notices, setting up a toll-free number, and 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, and/or web posting. Costs may also include the purchase of services of a forensic expert.

As noted in the final PRA analysis, the estimated annual cost burden for all entities subject to the final rule will be approximately \$795,235.

E. Steps the Agency Has Taken to Minimize Any Significant Economic Impact on Small Entities, Consistent With the Stated Objectives of the Applicable Statutes, Including the Factual, Policy, and Legal Reasons for Selecting the Alternative(s) Finally Adopted, and Why Each of the Significant Alternatives, if any, Was Rejected

In drafting the final rule, the Commission has made every effort to avoid unduly burdensome requirements for small 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. Moreover, as discussed above, the Commission has modified the final rule's requirements for timing and method of notice in several ways that will also reduce the burden on small entities.

Two commenters expressed concern that the effective compliance date of 30 calendar days from the date of publication of this final rule would not allow covered entities sufficient time to come into compliance. In response, the Commission notes that the effective compliance date is mandated by the Recovery Act. Moreover, as discussed above, the Commission believes that in many instances the rule will apply to entities that already have obligations to provide notification of data breaches under certain state laws covering medical breaches. As a result, these entities can build upon their existing programs in order to come into compliance with this final rule. Nevertheless, the Commission has determined that it will use its enforcement discretion to refrain from imposing sanctions for failure to provide the required notifications for breaches that are

discovered before [insert date 180 days after date of publication in the FEDERAL REGISTER].

The Commission is not aware of additional methods of compliance that will reduce the impact of the final rule on small entities, while also comports with the Recovery Act.

VI. FINAL 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 adds a new Part 318 to title 16 to the Code of Federal Regulations, to read as follows:

PART 318 – HEALTH BREACH NOTIFICATION RULE

Sec.

318.1 Purpose and scope.

318.2 Definitions.

318.3 Breach notification.

318.4 Timeliness of notification.

318.5 Method of notice.

318.6 Content of notice to individuals.

318.7 Enforcement.

318.8 Effective date.

318.9 Sunset.

Authority: Pub. L. No. 111-5, 123 Stat. 115 (2009).

§ 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, Pub. L. No. 104-191, 110 Stat. 1936, as defined in 45 C.F.R § 160.103.

(c) HIPAA-covered entity means a covered entity under the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936, as defined in 45 C.F.R § 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) 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 website; or

(ii) in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside.

Such a notice in media or web posting shall include a toll-free phone number, which shall remain active for at least 90 days, where an individual can learn whether or not the individual's 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 website.

§ 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, website, 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 [insert date 30 days after date of publication in the FEDERAL REGISTER].

§ 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.