

**America's Health
Insurance Plans**

601 Pennsylvania Avenue, NW
South Building
Suite Five Hundred
Washington, DC 20004

202.778.3200
www.ahip.org



May 29, 2009

Submitted Electronically at: <https://secure.commentworks.com/ftc-healthbreachnotification>

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: Health Breach Notification Rulemaking
Project No. R911002

Dear Sir or Madame:

I am writing on behalf of America's Health Insurance Plans (AHIP) to offer comments in response to the proposed regulations published in the *Federal Register* on April 20, 2009. (74 Fed. Reg. 17914.) The proposed regulations address the breach notification requirements under section 13407 of Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA)¹ intended for Personal Health Record (PHR) vendors and similar entities that are not covered by the Health Insurance Portability and Accountability Act (HIPAA).

America's Health Insurance Plans (AHIP) is the national association representing approximately 1,300 health insurance plans that provide coverage to more than 200 million Americans. Our members offer a broad range of health insurance products in the commercial marketplace and also have demonstrated a strong commitment to participation in public programs.

AHIP supported the health information technology and privacy provisions contained in the ARRA, and we believe the statutory requirements set a solid framework on which Health Insurance Portability and Accountability Act (HIPAA) covered entities and their business associates can design systems and processes to better protect individuals' health information. Many of our members are HIPAA covered entities and will be governed by the data breach regulations and guidance issued by the U.S. Department of Health and Human Services (HHS). Our members are dedicated to ensuring the privacy and security of their customers' data.

¹ This section of the law is also referred to as the "Health Information Technology for Economic and Clinical Health Act" or "HITECH Act."

May 29, 2009

Page 2

We are commenting on the FTC's proposed regulations to help ensure consistency between the parallel requirements for the different entities regulated by Title XIII of the ARRA. AHIP supported the statutory requirements that establish temporary breach notifications for PHR vendors and other non-HIPAA covered entities. We believe that consumers who purchase or use PHR products and services should receive notification if their identifiable, unsecured health information is breached.

Our comments below raise several issues and include our recommendations for addressing them in the final regulations. We have organized our comments and recommendations by topic headings that relate to the areas discussed in the proposed regulations.

Definitions

Issue 1: The proposed regulations solicit public comments about whether entities may have "access" to data, but the access does not constitute a breach because the data has not been "acquired."

Discussion 1: Section 318.2 defines a "breach of security" as the acquisition of unsecured PHR identifiable health information of an individual in a PHR without the authorization of the individual. The definition explains that unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the PHR vendor, PHR related entity, or the third party service provider that experienced a breach has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition. The preamble to the regulations lists one scenario in which access to data has occurred but no acquisition has taken place (and thus no breach notification was required) as the result of an employee inadvertently accessing an incorrect database. (74 Fed. Reg. 17915.)

Entities that use electronic systems frequently need technical support to investigate or correct technical issues. It would be helpful for the preamble to the final regulations to provide additional, practical examples of situations in which persons or entities may have "access" to data in the normal course of business (e.g., a technician accesses data while providing technical support), but no breach has occurred because the data has not been "acquired" (e.g., a technician views, but does not remove, electronic data in a system). These examples should also highlight when data is "acquired" and a data breach has occurred (e.g., a technical support contractor steals PHR identifiable health information by downloading it to a portable device).

Recommendation 1: The preamble and the final regulations should provide practical examples to illustrate situations in which: (1) data has been "accessed" but no breach has occurred; and (2) data has been "acquired" and a data breach has occurred.

May 29, 2009

Page 3

Issue 2: The FTC should explain in regulations and guidance how the HITECH definition of “breach of security” will be interpreted.

Discussion 2: Section 13407 of the statute, Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Entities, sets out the statutory definition for a breach of security.² The preamble explains that an entity that experiences a breach is in the best position to determine whether unauthorized acquisition has taken place. (74 Fed. Reg. 17915, 17916.) Essentially, the regulation creates a rebuttable presumption that unauthorized persons have acquired information if they have access to it, unless evidence shows that the information was not or could not reasonably have been acquired. (74 Fed. Reg. 17915, 17916.)

We support the rebuttable presumption and propose as an additional element that the agency include a “harm standard” as a threshold for providing notification. Such a standard would mean that no notification is required when no reasonable likelihood of harm to an individual exists (e.g., no reasonable likelihood of harm resulting from identity theft or other unlawful conduct) because information was not acquired. We believe adopting an additional threshold of a harm standard would better clarify how the FTC will apply the definition of breach in practical situations.

Recommendation 2: The final regulations should: (1) adopt a rebuttable presumption that unauthorized persons have acquired information if they have access to it, unless evidence shows that the information was not or could not reasonably have been acquired; and (2) use a threshold “harm standard” when evaluating whether a breach of protected health information has actually occurred.

Issue 3: The final regulations should more clearly define the term “PHR related entity.”

Discussion 3: Proposed regulation §318.2(f) defines “PHR related entity” to mean:

- [A]n 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

² The term is defined as, “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.”

May 29, 2009

Page 4

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

It would be helpful for the final regulations to explain what entities would be covered by §318.2(f)(3). Individual consumers who have a PHR can populate their own data into a PHR, can authorize any individual or entity to access their PHR information electronically (e.g., a family member or friend), and can ask persons or entities to send information to the PHR (e.g., a family member). Individual consumers can also give information from a PHR to anyone in paper form (e.g., to a personal care representative). We do not believe that the statute or the regulations intend to require the FTC to regulate persons who or entities that access PHR information in these situations.

We support the ability of consumers to participate in constructing PHR information and adding information to the PHR that they believe is pertinent to their health and care. However, we caution the FTC on defining (f)(3) so broadly that it encompasses unintended persons or entities.

Recommendation 3: In the final regulations, §318.2(f)(3) should read as follows (plain font text is newly added text; strikethrough text is deleted text):

“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) Electronically ~~Accesses information in a personal health record~~ without an individual’s authorization ~~or knowingly sends information to a personal health record~~ as part of its routine business operations.**

Notices to Individuals, the Media, and the FTC

Issue 4: The preamble and the final regulations should provide more information about the requirements for providing notices to the media and the FTC.

Discussion 4: The proposed regulations contain two requirements for notifying the media: (1) providing a substitute notice to an individual whose information was included in a data breach pursuant to §318.5(a)(4)(B) by notifying major media in geographic areas where the affected individuals likely reside; and (2) providing notice to prominent media outlets serving a state or

May 29, 2009

Page 5

jurisdiction if the unsecured PHR identifiable health information of 500 or more residents of a state or jurisdiction is reasonably believed to have been acquired during a breach pursuant to §318.5(b).

When providing the substitute notice, it may be difficult for an entity to determine where “affected individuals likely reside.” It can be unreasonable for an entity to notify all major U.S. media outlets simply because one or more individuals affected by a breach moved without providing current contact information to the PHR vendor or PHR related entity. We recommend that entities in these circumstances be permitted to use reasonable discretion under the circumstances.

In addition, §318.5(b), requires an entity to notify the media if the unsecured PHR identifiable health information of 500 or more residents of a state or jurisdiction is reasonably believed to have been acquired during a breach. Section 318.5(c) also requires notice to the FTC in such a situation. The final regulations should define the term “jurisdiction” (e.g., to include the District of Columbia; U.S. territories such as the U.S. Virgin Islands) and clarify that it is not meant to include broad geographic regions in the U.S. encompassing more than one state (e.g., the east coast or the northwest corridor).

Also, the final regulations should allow a PHR vendor, a PHR related entity, or a third party service provider to use reasonable discretion when calculating “if ten or more individuals cannot be reached” (as required by §318.5(a)(4)) and how the unsecured PHR identifiable health information of “500 or more residents of a state or jurisdiction” is reasonably believed to have been acquired during a breach (as required by §318.5(b)) (e.g., if a data breach by a third party service provider affects the customers of two or more PHR vendors).

Recommendation 4: The preamble and the final regulations should explain that PHR vendors and PHR related entities have reasonable discretion in: (1) determining where “affected individuals likely reside” under §318.5; and (2) calculating the number of individuals involved in a data breach, as long as the entities can justify a reasonable basis for the calculations used. The final regulations should also include a definition for the term “jurisdiction” and indicate that this term includes the District of Columbia.

Issue 5: Regulation §318.3(b) proposes a process that may delay, rather than expedite, notices to consumers, the media, and the FTC when a breach of security occurs.

Discussion 5: Proposed regulation §318.3(b) would require a third party service provider to give notice of a breach of security to a senior official at the PHR vendor or PHR related entity to which it provides services and obtain an acknowledgment from the senior official that the notice was received. We are concerned that this proposed regulation can divert time and resources of

May 29, 2009

Page 6

the PHR vendor or PHR related entity from sending prompt notifications to individuals, the media, and the FTC.

If a breach of security occurs, the PHR vendor or the PHR related entity should work expeditiously with the third party service provider to investigate the breach and provide appropriate notices. Waiting for an official acknowledgement from a senior manager at a PHR vendor or PHR related entity can delay such important activities.

Recommendation 5: In the event of a breach of security, the final regulations should require a third party service provider to: (1) provide notice to a senior official at the PHR vendor or PHR related entity to which it provides services; and (2) retain evidence that the notice was sent. The preamble to the final regulations should encourage third party service providers to verify (e.g., through oral, written, or electronic communication) that the PHR vendor or the PHR related entity has received the notice and will provide any required notifications.

Issue 6: Proposed §318.5(c) should be revised to: (1) allow PHR vendors and PHR related entities adequate time to conduct an investigation following a suspected breach of security; (2) set an annual, defined date by which PHR vendors and PHR related entities should submit a data breach log to the FTC; (3) allow corporate entities to define how information is reported to the FTC; and (4) clarify that PHR vendors and PHR related entities should not report individuals' personal data to the FTC.

Discussion 6: When a breach of security is suspected, PHR vendors and PHR related entities will need adequate time to conduct an investigation and assess whether a breach of security has actually occurred, and, if so, what information was breached and what individuals are affected. We are concerned that requiring PHR vendors and PHR related entities to notify the FTC no later than 5 business days following the date of discovery of a breach will not allow sufficient time in all situations to conduct an investigation. This can result in premature notices to the FTC based on incomplete information about the surrounding facts and circumstances.

Proposed §318.5(c) also allows PHR vendors and PHR related entities to submit an annual log to the FTC containing information about breach of security situations involving the unsecured PHR identifiable health information of fewer than 500 individuals. This requirement can be interpreted as establishing a "rolling date" for reporting that varies by entity and begins when an entity experiences its first annual breach of security that affects fewer than 500 individuals. A single reporting date would ease the FTC's responsibility for compliance oversight and administration. As an alternative to the proposal, we recommend that the final regulations establish a single reporting date for all PHR vendors and PHR related entities. The log may be

May 29, 2009

Page 7

sent 30 or 60 days after the end of the calendar year documenting the breaches from the preceding year.

We also recommend that future regulations and guidance allow corporate entities the ability to define how information is reported to the FTC. For example, if a corporate entity owns a number of wholly-owned subsidiaries or has affiliated entities, that corporate entity is in the best position to decide whether one corporate report should be sent, or whether individual entities (e.g., subsidiaries) should submit individual reports.

Finally, the preamble to the regulations explains that the FTC will be developing a form that will be posted on the agency's website and used by entities to provide both immediate and annual notices to the agency. When developing the report form, we encourage the FTC to include a clear statement that no PHR identifiable information should be reported.

Recommendation 6: Proposed §318.5(c) should be revised to require PHR vendors and PHR related entities to: (1) report a breach of security to the FTC no later than 5 business days following the vendor's or entity's confirmation of the facts and circumstances indicating that a breach occurred; (2) submit a log of data breaches involving fewer than 500 individuals per instance at a set number of days following the end of a calendar year; (3) allow corporate entities to determine how to compile and report information to the FTC; and (4) clarify that PHR vendors and PHR related entities should not report individuals' personal data to the FTC.

State Laws

Issue 7: PHR vendors and PHR related entities may face challenges complying with both federal and state laws and regulations related to breaches of data security.

Discussion 7: Different state requirements for notifying affected individuals following a data breach (i.e., differences between the federal requirements and state laws and regulations) may create challenges for PHR vendors and PHR related entities.

§§13402 and 13407 of the ARRA sets out the federal breach notification requirements, which includes notice to affected individuals within 60 calendar days following the discovery of a breach. By way of example, New Jersey law³ requires any business that conducts business in the state, or any public entity that compiles or maintains computerized records that include personal information, to disclose a breach of security of computerized records to residents whose information was included in the breach. Before notifying individuals under the New Jersey law,

³ N.J. Stat. Ann. §§56:8-163.

May 29, 2009

Page 8

however, the business or entity must first report the breach of security and any information pertaining to the breach to the New Jersey Division of State Police and then must wait to receive notification from that agency that notice to individuals will not compromise any law enforcement investigation.

In reviewing the federal statute and the New Jersey requirements, it is foreseeable that PHR vendors and PHR related entities may be in a situation where federal law and regulations require them to send notice to individuals within 60 calendar days following a breach, but the state law enforcement agency has not provided clearance to issue the notice under state law. Another possible outcome is that the differing federal and state requirements may result in duplicate notices being sent to individual consumers.⁴

Recommendation 7: The final regulations should explain how PHR vendors and PHR related entities should handle situations where federal and state laws or regulations impose differing data breach requirements, such as state requirements that provide standards that are different from the federal requirements for notifying affected individuals following a data breach.

Relation to HHS Security Guidance

Issue 8: Section 318.2(h) should reference the HHS security guidance.

Discussion 8: In defining the term “unsecured,” §318.2(h) mirrors the statutory language by explaining that PHR identifiable information is not protected unless an entity uses a technology or methodology specified by the HHS Secretary in guidance. The proposed regulation then sets out a meaning for the term if the guidance is not issued.

HHS released the security guidance on April 17, 2009 and solicited public comments in response. HHS subsequently published the guidance in the *Federal Register* on April 27, 2009. (74 Fed. Reg. 19006.)

Recommendation 8: The final regulations should incorporate a specific reference to the HHS security guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, and indecipherable to unauthorized individuals.

⁴ Massachusetts law also includes requirements for providing consumers notices following a data breach that are different from the federal HITECH provisions, including specific content requirements. Clarification would be helpful to explain whether entities would be required to send two notices to comply with the state and federal data breach requirements, or whether the federal law will govern. *See*, Mass. Gen. Laws ch. 93, §3 and ch. 93H, §3.

May 29, 2009

Page 9

Jurisdiction

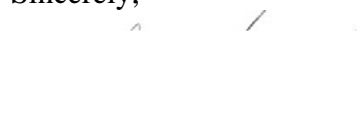
Issue 9: The preamble and the final regulations should clarify whether Health Information Exchanges (HIEs) would come under the FTC's jurisdiction.

Discussion 9: As the health care industry works toward developing a nationwide health information network, HIEs have emerged as a new type of entity that has the ability to collect, store, or exchange individual's health information. In some contexts, HIEs are business associates of HIPAA covered entities. However, HIEs have the technical ability to exchange information with non-HIPAA entities or business associates (e.g., where an HIE receives information from a PHR vendor).

Recommendation 9: The preamble and the final regulations should explain that in some situations HIEs will be subject to the FTC's jurisdiction (e.g., where an HIE receives information from a PHR vendor), while in other situations, HIEs will be subject to HHS' jurisdiction and enforcement (e.g., when the HIE acts as a business associate to a HIPAA covered entity).

Thank you for the opportunity to comment on these important issues.

Sincerely,


Marilyn Zigmund Luke
Senior Regulatory Counsel