June 1, 2009

Submitted Electronically at: https://secure.commentworks.com/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 Madam:

Molina Healthcare, Inc. (MHI) is writing 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) intended for Personal Health Record (PHR) vendors and similar entities that are not covered by the Health Insurance Portability and Accountability Act (HIPAA).

Molina Healthcare, Inc. is a multi-state managed care organization that arranges for the delivery of health care services to persons eligible for Medicaid, Medicare, and other government-sponsored programs for low-income families and individuals. Molina Healthcare's ten licensed health plan subsidiaries in California, Florida, Michigan, Missouri, Nevada, New Mexico, Ohio, Texas, Utah and Washington currently serve approximately 1.3 million members.

Molina supports 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. Molina is committed to ensuring the privacy and security of our members.

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. Molina supports 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, whether the health information was maintained by a HIPAA covered entity, its business associate, or a non-HIPAA entity such as a PHR vendor, a PHR related entity, or a third party service provider.

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

Comment 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."

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 when 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 from 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).

The FTC should include examples in the preamble and the final regulations to illustrate when: (1) data has been "accessed" but no breach occurs; and (2) data has been "acquired" and a data breach results.

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

We support the rebuttable presumption, and propose as an additional element that the agency include a "harm standard." Such a harm standard would mean that no notification is required when no reasonable harm to an individual exists (e.g., no reasonable harm of 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.

The FTC 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.

Comment 3: The final regulations should more clearly define the term "PHR related entity."

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 authorize any individual or entity to access their PHR information electronically (e.g., a family member or friend); they can also send information to the PHR. Individual consumers can also send or 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.

In addition, in some applications, individual consumers can populate data in the PHR. This means that individuals can place data into a PHR that they received from another source (e.g., a family member's laboratory report). The originator of the data would likely have no knowledge that information given to an individual has been added to or sent to a PHR.

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.

The FTC 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 ~~A~~accesses information in a personal health record as part of its routine business operations or knowingly sends information to a personal health record as part of its routine business operations.

Notices to Individuals, the Media, and the FTC

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

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.

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).

The FTC preamble and the final regulations should explain that PHR vendors and PHR related entities have 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 state that this term means the District of Columbia.

Comment 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.

We are concerned that this proposed regulation can divert time and resources of 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 stall or delay such important activities.

The FTC should require in the event of a breach of security, third party service providers 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 have received the notice and will provide any required notifications**.**

Comment 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 to conduct an investigation in all situations. 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 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 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.

The FTC should revise the proposed §318.5(c) 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 that a breach occurred; (2) submit a log of data breaches involving less than 500 individuals per instance at the same time following the end of a calendar year; (3) allow corporate entities to determine how to compile and report information to the FTC; and (4) exclude PHR identifiable information from any forms or reports sent to the FTC.

State Laws

Comment 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.

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.

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.

The FTC 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

Comment 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.)

The FTC 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.

Jurisdiction

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

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).

The FTC should explain in the preamble and the final regulations that in some situations HIEs will be subject to the FTC's jurisdiction (e.g., where an HIE receives information from a PHR vendor). However, in some 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,

Timothy C. Zevnik, CIPP/G
Privacy Official & Director HIPAA Program
Molina Healthcare, Inc.