To: The Federal Trade Commission

From: Kathleen Ojala, Associate Director, Compliance Coordination; Jennifer Cironi, Privacy Officer; Tremayne Smith, Data Security Manager

MEMO

Subject: Commentary to FTC rules related Health Breach Notification Rulemaking, Project No. R911002

Date: May 20, 2009

We respectfully submit the following in response to the Notice of proposed rule making and request for public comment related to vendors of personal health records and related entities, and associated breach notification requirements.

The Commission is seeking extensive commentary. We have commented on select issues as follows:

Proposed Section 318.1: Purpose and Scope

We agree that the proposed rule should not apply to HIPAA covered entities or to an entity's activities as a business associate of a HIPAA covered entity. We request that the Commission further clarify its intent regarding employee health records of a HIPAA covered entity. In its definition of Protected Health Information[1], HIPAA excludes individually identifiable health information in employment records held by a covered entity in its role as employer, as well as records covered in FERPA. It is our belief that the FTC does not intend to include employee health records of a HIPAA covered entity, in its definition of PHR nor that a HIPAA covered entity's management of employee health records will render the covered entity a PHR vendor. In addition, we seek the Commission to clarify that records covered under FERPA are excluded from 318.1.

Proposed Section 318.2: *Definitions*

The definition of *Personal Health Record*[2] should be expanded to include paper records. Personal health record is defined as 'electronic record,' only. We recommend that the definition be expanded to include print media. It is possible that a PHR vendor will use print records, either downloading information entrusted to the PHR vendor, or accepting fax or mailed copies of medical records, scanning those records, and then uploading the records into their system. Although we anticipate the vast majority of the PHR vendors' records to be electronic, protection of the consumer's privacy rights requires inclusion of print media in the definition of PHR.

The definition of *Third Party Service Provider* should be clarified. The proposed regulation defines "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

---

[1] 45 CFR § 160.202 *Protected Health Information* (2)(iii)

[2] A Personal health record is defined as "an electronic record of PRH 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."

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."[3]

The definition of third party service provider in the proposed rule does not contemplate the role of researcher access to PHR information. HIPAA covered entities extend significant resources and have significant requirements as far as research access to protected health information. One can contemplate researchers bypassing HIPAA covered entities and pursuing PHRs for health research purposes. If not bypassing HIPAA covered entities, then at least approaching PHRs for health research opportunities the aggregate data would likely represent.

Changing the conjunction in the definition of a third party service provider between numbers 1 and 2 to "or" rather than "and" would change the definition such that it would apply to researchers. A researcher could potentially access, maintain, record, store or otherwise hold, use or disclose unsecured PHR identifiable health information. However, researchers would not access PHR data in connection with offering or maintaining the PHR. Therefore, the writers of this response suggest changing the conjunction between the sentences to "or" which would likely cover any research activities.

Proposed section 318.3: Breach Notification Requirement:

Section 318(a) requires that a vendor of PHR and PRH 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. We suggest that the presumption exist that that all consumers served by the PHR vendor and PHR related entities are U.S. citizens and U.S. residents unless the entity has clear information to the contrary. The Commission believes that some entities will not gather consumer mailing addresses (as discussed in Proposed Section 318.5 (a)(3) Substitute Notice), and it is also likely that citizenship of the consumer will not be known. In order to provide the greatest consumer protection, a presumption of U.S. citizenship or residency should exist.

Proposed Section 318.5: Methods of Notice (a)(3)

Substituted notice allows for a "conspicuous"[4] posting on the webpage of the entity. We respectfully ask the Commission to adjust the duration of the posting from 6 months to 45 days. As a covered entity, our limited experience with an electronic medical record, accessible by patients, shows a bimodal pattern of access. Some patients access their electronic medical record regularly; coinciding with a visit with their health care provider. The other group of patients open their account, but then fail to access it again despite additional encounters. We believe that a posting of a data breach notice on the website of the vendor for 6 months will unduly alarm consumers (who may themselves have been victimized), each time the vendor's webpage or landing page is accessed. Additionally, posting breach information for prolonged period may stimulate new breach attempts by parties predisposed to capitalizing upon perceived weaknesses in vendor systems. Our opinion is that greatest immediate damage to most consumers for a PHR breach stems from the breach of financial information. Media broadcasts have shown that financial fraudsters act upon financial information immediately. Notice from a vendor 3-6 months after the breach does not protect the consumer/victim. We do recommend that a vendor of PHRs maintain, as a matter of routine business, a dedicated contact line for consumers concerned about data breaches and the security of their information. Consumers who missed the initial breach notice efforts can seek further information through this dedicated line.

[3] 16 CFR § 318.2(g).
[4] 13402(e)(1)(B) of the Recovery Act

Paperwork Reduction Act

In response to the Commissions invitation for comment on: (1) whether the proposed collection of information is necessary for the proper performance of the FTC, including whether the information will have practical utility:

We suggest that in addition to breach notification the FTC adopt standards to promote consumer protection via prevention of data breaches. The two primary harms arising from data breaches is the risk of financial harm, and the invasion of privacy related to a consumer's health condition. The PHR vendors will 'interact' with personal health records. To the degree the vendor of the PHR abstains from collecting financial information (including social security numbers (SSNs)), the potential resultant damages decreases significantly. As the Commission is proposing instructing vendors on methods of breach notification, we urge the Commission to instruct the vendors to inform their consumers, conspicuously, of the risks of breach and resultant possible damages at the time the vendor/consumer relationship is being formed.

Many covered entities collect, store and use SSNs primarily for billing for treatment rendered the patient. SSNs are used by CMS as the primary method of patient identification for payment purposes. Unfortunately, SSNs are used as identifiers in many circumstances, and extricating the SSN and use of the SSN from covered entity's systems is impracticable.

If the vendor of the PHR were disincentivized to collect SSNs, and other financial data elements, the consumer will ultimately be better protected. One suggestion for disincentive is to require the vendors to prominently post the risk of a data breach to prospective and ongoing customers, and the resultant cost to the consumer if his/her financial data were breached. Per the Commission's analysis, there is a 1.2% chance of a data breach by any one of the PHR vendors (11 breaches/year/900 entities). The resultant cost to the consumer includes identity theft monitoring and remediation of breached financial accounts. The Commission has extensive experience with the associated cost of harm related to identity theft and PHR vendors should be persuaded to use the Commission's experience with identity theft mitigation to protect future harms to consumers.