Sonnenschein
SONNENSCHEIN NATH & ROSENTHAL LLP

1301 K Street, N.W.
Suite 600, East Tower
Washington, D.C. 20005-3364
202.408.6400
202.408.6399 fax
www.sonnenschein.com

Marc J. Zwillinger
202.408.9171
mzwillinger@sonnenschein.com

June 1, 2009

VIA ELECTRONIC SUBMISSION

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:

On behalf of our law firm, and consistent with the Federal Trade Commission's ("FTC") April 16, 2009 notice of proposed rulemaking and request for public comment, Sonnenschein Nath & Rosenthal LLP ("Sonnenschein") is writing to provide comments on the FTC's Health Breach Notification Rule. Given the significant effect the breach notification requirements could have on personal health record ("PHR") vendors and PHR related entities, we appreciate your consideration of our comments, as set forth below.

Health Breach Notification Rule Creates Conflicts with State Law

PHR vendors and PHR related entities (as well as other persons and entities) currently are obligated to comply with state breach notification laws in the event of a breach of personal information or sensitive personal information. In addition to defining what constitutes sensitive personal information, some state breach notification laws dictate what must, and significantly, what must *not* be included in the notification to the individual. For example, the Massachusetts breach notification law prohibits the inclusion of information concerning the nature of the breach, unauthorized acquisition or use or the number of residents affected by the breach.[1] In contrast to the Massachusetts' law, the Health Breach Notification Rule currently states that the notice of a breach provided to individuals must include an explanation of what happened and a description of the types of unsecured PHR identifiable health information that were involved in the breach. Thus, where both laws are triggered, such as with payment information associated with payment for medical services, the Massachusetts law and the proposed Health Breach Notification rule are irreconcilable, making it impossible to comply with both sets of laws in the

[1] Massachusetts General Law Chapter 93H.

event both PHR identifiable health information and sensitive personal information of Massachusetts residents are the subject of the breach.

Need for Multiple Breach Notices Still Exists

Given current obligations under state breach notification laws, PHR vendors and PHR related entities still anticipate having to send multiple notices to individuals upon discovery of a single breach, and that there will be circumstances under which the notice required by the proposed Health Breach Notification rule will not satisfy notice obligations under state law. More specifically, certain state laws include requirements that the notice include specific information that would not be applicable to residents in all states, and would not be included in a notice that complied only with the proposed Health Breach Notification rule's requirements. For example, Maryland state law requires that the notice to individuals contain the contact information for the Maryland Attorney General's Office.[2] In addition, Massachusetts' law requires the notice to include a statement regarding a consumer's right to obtain a police report, how a consumer may request a security freeze, and any fees required to be paid to any of the consumer reporting agencies.[3] A notice that complied only with the proposed Health Breach Notification rule's breach notification requirement would not include the information required under either the Maryland or Massachusetts state laws, and thus, would not satisfy the notice obligations under state law. The only remedy to the situation is to send multiple breach notices, or to send a complicated addendum to each notice containing the individual requirements of each state and federal law, either of which may cause customer or patient confusion.

Time Within Which Notification to FTC Must Be Made Should be Extended

The proposed Health Breach Notification rule requires that notice be made to the FTC as soon as possible, but no later than five business days following the discovery of the breach. Given the necessary steps that must be taken to determine the factual circumstances surrounding a breach, including a determination of the data elements breached and the number and identity of individuals affected, notification to the FTC within five business days is not reasonable, and thus, we request that the FTC reconsider the specific time frame within which it will require PHR vendors and PHR related entities to notify it of a breach. If notification to the FTC of a breach is required within five days, it is unlikely that this notification will provide the details necessary to make the notification substantively significant. Rather, it will contain information based on theories or assumptions that may turn out to be incorrect. For example, though a company may determine immediately that an unauthorized individual gained access to certain data systems, a detailed forensic examination may be necessary to determine the extent of the compromise and the specific data elements that were put at risk. We have counseled clients on

---

2 Md. Comm. Law Code Ann. 14-3504.

3 Massachusetts General Law Chapter 93H.

breach notification since the first state breach notification statute was passed in California. Invariably, we have found that the information (and the confidence level about the information) changes significantly over the first 7-10 days following a breach. To require a company (who in many cases is a victim of a third-party hacking attack) to provide detailed notification to the FTC in writing within 5 business days following the discovery of a breach is unfair to the victim and would not likely protect consumers. The requirement is unfair to the victim because: (1) any written notification submitted to the FTC will likely play a role in subsequent civil litigation given the increase in plaintiffs' claims related to breaches; (2) where state laws require breach notification to be given to individuals without undue delay, companies required to provide notice to the FTC within five business days will also be forced to provide immediate breach notification to individuals immediately following the FTC notice or risk facing a subsequent inquiry to explain any further delay; and (3) companies may then be forced to send an additional corrective notice to individuals, thereby resulting in (potentially significant) increased notification costs. This will ultimately harm consumers, because companies may, in good faith, provide incorrect or incomplete information in the initial notification due to the time pressure which could cause consumer confusion or unnecessary consumer reactions where overnotification is provided out of an abundance of caution

Based on our lengthy experience with data breaches, a 10-day period for providing notice to the FTC would be more appropriate and would allow PHR vendors and PHR related entities the opportunity to take steps necessary to investigate the circumstances surrounding the breach, mitigate any potential harm, and provide accurate, timely notifications to both the FTC and to consumers.

Website Posting Should be Limited to a Reasonable Period of Time

In its proposed Health Breach Notification rule, the FTC requires PHR vendors and PHR related entities to post the breach notice on their websites for a period of six months where more than 10 individuals cannot be contacted based on their information on file. This notice must include a toll-free number that individuals can call to learn whether their information may have been subject to the breach. We believe that requiring the notice to be posted for a period of six months, and thus, maintaining a dedicated line for related inquiries for 6 months, is an unreasonable period of time because the burden it places PHR vendors and PHR related entities is not commensurate with the potential advantages to individuals. Specifically, if a PHR vendor or PHR related entity lacks sufficient contact information for an individual, it is unlikely that it maintains a current or ongoing relationship with that individual. Therefore, although possible, it is unlikely that these individuals would be see a notice that was posted for 6 months, but not see it (or hear about it in the press) if the notice were only posted for 30 or 60 days.

We recommend that the FTC require PHR vendors and PHR related entities to post notice of a breach on their websites for a period of no less than 30 days and then allow them to make a

reasonable determination whether they are getting sufficient call traffic to maintain the notice and toll-free lines for an additional 30 day period. Thirty days is a reasonable period of time because it provides individuals who may not have received the written notice the opportunity to learn of the breach, but does not remain on the website so long as to confuse people by making them think that the breach is a new or additional breach. Such a framework would also allow entities that are getting little or no call traffic to close their toll-free lines, while others with significant call volume would extend the period of notice.

* * * * * * * * *

On behalf of our clients and our firm, we appreciate your consideration of our comments. If you have any questions, please contact me at 202-408-9171, or my colleagues, Rebecca Fayed, at 202-408-6351, or Lisa Branco, at 202-408-3936.

Sincerely,

/s/

Marc J. Zwillinger