WebMD
111 Eighth Avenue
7th Floor
New York, NY 10011
212-624-3700 Phone
212-624-3773 Fax
www.webmd.com

June 1, 2009

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

Re: Health Breach Notification Rulemaking, Project No. R911002

Dear Sir or Madam:

WebMD Health Corp. ("WebMD") appreciates this opportunity to comment on the Federal Trade Commission's ("FTC's" or the "Commission's") proposed Health Breach Notification Rule ("Proposed Rule"), implementing Section 13407 of the American Recovery and Reinvestment Act of 2009 ("ARRA").[1] WebMD is the leading provider of health information services for consumers, healthcare professionals, employers, and health plans through public and private portals.

Through its subsidiary, WebMD LLC, WebMD provides a consumer-directed health portal (the "WebMD Consumer Portal") that provides visitors with health and wellness related information, tools and applications in a variety of content formats. The WebMD Consumer Portal includes unique features that help consumers check symptoms, locate physicians, assess personal health status, receive e-newsletters and alerts, and participate in online communities with peers and medical experts. Through the WebMD Consumer Portal, WebMD reaches more than an average of 60 million unique users each month.

Through another subsidiary, WebMD Health Services Group, LLC, WebMD provides a leading brand of private health and benefits portals ("WebMD Health and Benefits Portal") that enable employees and plan members to make more informed benefit, treatment and provider decisions. Through a single, secure gateway, individuals can access their personal health information, which is integrated with medical claims and plan-specific data within WebMD's personal health record ("PHR"). WebMD offers the WebMD Health and Benefits Portal to members and employees of more than 130 of the largest corporations and health plans.

Both the WebMD Consumer Portal and the WebMD Health and Benefits Portal offer PHR capabilities in which individuals can create personal accounts and maintain their health information. Through the WebMD Consumer Portal, WebMD is a direct provider of PHRs to the public. The WebMD Health and Benefit Portal enables members of participating health plans to manage their personal health information through a PHR typically sponsored by HIPAA covered health plans. WebMD functions as a business associate to the health plans or sponsors that it supports through the WebMD Health and Benefits Portal.

---

[1] Health Breach Notification Rule, 74 Fed. Reg. 17,914 (Apr. 20, 2009).

WebMD is committed to protecting the privacy and security of individuals' health information and appreciates the importance of having a fair and effective federal health breach notification rule. WebMD respectfully requests that the FTC consider the following comments when promulgating its interim final regulations on the temporary breach notification requirements for vendors of personal health records ("PHR vendors").

I. Potential for Entities to Serve a Dual Role as a PHR vendor and a Business Associate

WebMD appreciates the FTC's recognition that the federal data breach provisions, as set forth under ARRA, may subject some entities to dual notification requirements—both as a PHR vendor and a business associate.[2] We have provided comments below regarding some of the possible implications associated with this dual role.

A. Proposed Sections 318.1 and 318.2(i)—Exclusion of Business Associates from the Definition of PHR Vendor

WebMD strongly supports the FTC's clarification that the Proposed Rule does not apply to HIPAA covered entities or their business associates.[3] We believe that the exclusion of an entity's activities as a business associate from the definition of PHR vendor is critical to ensuring that entities that offer PHRs in a business associate capacity are not subject to two different breach notification requirements – those implemented by the FTC and by the Department of Health and Human Services ("HHS") – for a single business activity.

Many providers of PHRs serve as business associates to health plans and other covered entities that sponsor PHRs for individual members and also qualify as vendors of PHRs because they maintain individuals' personal health records outside of a business associate capacity. In the event that a breach occurs, it will be important to a PHR vendor's successful implementation of the HHS and FTC breach notification standards to have clear guidance on which rules apply. By clearly stating that the FTC rule will not apply to business associate activities (because there the HHS notification rules will apply), the FTC has helped ensure that consumers will not receive duplicate notices for a single security incident. Apart from the administrative difficulties that might arise from two separate entities providing notifications, affected individuals' receipt of multiple notifications of a single incident would likely unnecessarily increase their anxiety and confusion surrounding a breach.

We believe that the FTC's clarification that the scope of these regulations do not apply to an entity's activities as a business associate to a HIPAA-covered entity is appropriate. Accordingly, we urge the FTC to finalize these provisions.

B. PHR Vendors as Business Associates

Section 13408 of ARRA requires that "each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record," enter into a business associate agreement with the covered entity. WebMD seeks clarification from the FTC that PHR vendors are required to enter into agreements with covered entities only to the extent that they maintain PHRs *on behalf of* the covered entity. WebMD believes that this approach is consistent with the intent of ARRA and other federal privacy laws. Under the HIPAA Privacy Rule, a "business associate" is defined as "person

---

[2] 74 Fed. Reg. at 17,915.

[3] *See* proposed Section 318.2(i) and 74 Fed. Reg. at 17,917.

who on behalf of...[a] covered entity...arrange[s], performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information..."[4] Accordingly, we do not believe that it is the intent of Congress that PHR vendors should be required to enter into business associate agreements with covered entities when a PHR is created on behalf of individuals, rather than as part of the activities of a health plan, even though the PHRs may be sponsored by a health care provider or plan. We request that the FTC clarify that where a PHR vendor is not performing a function or activity on behalf of a covered entity, it is not a business associate.

C. Portability

Also related to the dual-role that some businesses may have under the federal breach provisions, WebMD seeks clarification regarding the application of the breach notification provisions when an individual decides to discontinue use of a PHR supported through a covered entity (i.e., when an individual switches employment or changes health insurance coverage) and subsequently elects to continue using the services of a PHR vendor directly. Regardless of whether an individual maintains a PHR through a health plan that engages a PHR vendor as a business associate or an individual works with the PHR vendor directly, the individual will receive notification in the event of a data breach. In the first circumstance, where the PHR vendor is a business associate and the HHS rules apply, the vendor will notify the covered entity who will in turn notify the individual. In contrast, when an individual directly uses the services of a PHR vendor that is not acting as a business associate, the vendor will be required, under the FTC rules, to provide direct notification to the individual.

WebMD encourages the FTC to clarify that entities are subject to the breach notification provisions based on the conditions under which an individual's information is maintained at the time of the breach. For example, if a breach occurs after an individual switches from maintaining their PHR identifiable health information through a health plan to maintaining such information directly with the PHR vendor, the PHR vendor notification requirements should apply.

D. Uniformity of FTC and HHS Breach Notification Rules

WebMD appreciates the FTC's intention to work with HHS to harmonize the agencies' respective breach notification rules. As a company that may have business components subject to the different rules, we urge the FTC and HHS to make these rules as uniform as possible. The goals of these rules are the same: to ensure that consumers are informed if their health information is at risk. Harmonizing the requirements issued by the two agencies will reduce administrative complexity for companies that may be subject to the two different sets of rules, and this, in turn, will greatly facilitate prompt notice to consumers in the event of any breach of their personal health information.

II. Notification Trigger

A. Proposed Section 318.2(a)—Breach of Security

Proposed Section 318.2 defines a "breach of security" as the unauthorized acquisition of "unsecured PHR identifiable health information of an individual in a personal health record."[5] It further introduces a rebuttable presumption whereby an unauthorized acquisition is

---

[4] 45 C.F.R. § 160.103 (2006).

[5] *See* proposed Section 318.2(a) and 74 Fed. Reg. at 17,915.

"presumed to include [an] unauthorized access to unsecured PHR identifiable health information unless a 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 have reasonably have been, any unauthorized acquisition of such information."[6] We agree with the FTC that the entity experiencing an unauthorized acquisition of unsecured PHR identifiable health information is in the best position to determine whether such access amounts to an unauthorized acquisition.

In light of the proposed presumption and the responsibility that the new federal breach provisions place on entities experiencing a "breach of security," WebMD seeks clarification from the FTC that notification is not required following a breach if there is no reasonable likelihood of harm to an individual. We believe that PHR identifiable health information should not be considered "acquired" for purposes of the data breach notification requirement, if there is no reasonable likelihood of harm to the individual. For example, if an IT employee downloaded the wrong file of PHR members to work through a software glitch, reported it to the appropriate supervisor and destroyed the file, there would likely be no reasonable risk of harm to the individual and the notification requirement in that instance should arguably not be triggered.

The purpose of the federal breach notification provisions is to inform individuals of security incidents in part so that they can be appropriately vigilant and take preventative measures to mitigate harm. That is why the notification letters must include instructions on steps that can be taken to help protect the individual. As many states have recognized in their state data breach notification requirements, there is little if any value in providing data breach notification where there is no reasonable likelihood of harm. Instead it results in unnecessary anxiety and confusion for the individual who receives the notification. For the PHR vendor, PHR related entity and third party service provider who are responsible for providing notification, it results in needless administrative costs and responsibilities. This is particularly true given the fact that under the federal breach provisions, entities are sometimes required to provide notification to individuals, the FTC and local prominent media outlets following a breach.

III. Proposed Section 318.4 – Timeliness of Notification

Proposed Section 318.4(b), states that "[t]he 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*."[7] It appears that FTC is cognizant that there may be unforeseen delays that would prevent a PHR vendor or PHR related entity from complying with the notice timing requirement and we commend FTC's acknowledgement of this issue. WebMD urges the FTC to provide further guidance on what, other than a determination by a law enforcement official that notice would impede a criminal investigation or cause damage to national security, constitutes sufficient evidence to justify a delay in providing notice as alluded to in proposed Section 318.4(b).

IV. Proposed Section 318.5(c)—FTC Notification

---

[6] *Id.*

[7] *See* proposed Section 318.4(b) (emphasis added).

WebMD is concerned that the five day timeframe in which the FTC must be notified of a breach involving more than 500 individuals is not sufficiently long to provide entities with adequate time to conduct a meaningful investigation. The information discovered in the first five days is at times incomplete and unreliable. We believe all parties will be better served if entities are given sufficient time to conduct a meaningful investigation before FTC notification is required.

V. Areas of Conflict Between Federal Breach Notification Requirement and State Security Breach Notification Laws

WebMD believes potential conflicts with state laws are important for the FTC to consider as it promulgates the final health breach notification rule. While state security breach notification laws are not specific to personal health records, they may be implicated if a PHR vendor, PHR related entity or third party service provider experiences a breach of security. Many of these state laws apply broadly to a person or entity that conducts business in the state and owns or licenses computerized data that includes personal information (which includes entities covered by the FTC Proposed Rule). Further, notice to an individual is required under the state laws if there is a breach of "personal information," which is generally defined to include an individual's name in combination with a sensitive identifier such as social security number, drivers license or other state-issued identification number and financial account number (e.g., credit card or debit card number).

The PHR identifiable health information maintained by PHR vendors, PHR related entities and third party service providers commonly at times include identifiers deemed "personal information" under the state laws. In the preamble to the Proposed Rule, the FTC indicated that "a security breach of a database containing names and credit card information, even if no other information was included" would be covered by the Proposed Rule.[8] Notably, that same breach also would be covered by all of the states and U.S. jurisdictions that have a security breach notification law. Because the breaches covered by the Proposed Rule also typically will require notifications under state laws, we have highlighted some of the key concerns for entities attempting to comply with these federal and state laws and requested guidance from the FTC on how entities should comply with both sets of provisions.

a. Proposed Section 318.6 - Content of Individual Notice Requirements

i. Clarification that a single federal/state notice may be issued upon discovery of a single breach

Proposed Section 318.6 describes the required content for notice provided to individuals, including a brief description of the breach and the types of unsecured PHR identifiable health information involved, steps individuals should take to protect themselves from potential harm, and so forth. We appreciate that these requirements are set forth in Section 13407(c) of ARRA and that the same requirements also apply to HIPAA-covered entities subject to the authority of HHS, but we urge the FTC to issue clarifying guidance as to how a PHR vendor or PHR related entity may comply with both state and federal law where the state required elements for individual notice differ from the federal requirements.[9]

---

[8] 74 Fed. Reg. at 17,916.

[9] Section 13407(c) of ARRA provides that the individual notice content requirements applicable to HIPAA covered entities at Section 13402(f) also apply to FTC-regulated entities "in a manner specified by the Federal Trade Commission." ARRA, Pub. L. 111-5, § 13402(f), 123 Stat. 115 (Feb. 17, 2009).

Many states impose requirements for the content of a notice to individuals affected by a breach that are consistent with Section 318.6 of the Proposed Rule, but there are several instances where a notice that complies with the federal law would not comply with state law. For example, some states require that a breach notice include advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports,[10] others require advice to report suspected incidents of identity theft to law enforcement agencies including the FTC,[11] and still others require inclusion of the contact information for all major national consumer reporting agencies.[12] In these circumstances, absent a clarification from the FTC that a single notice is permitted under federal law, a PHR vendor or a PHR related entity may be required to send a federal and a state notice about the same breach to an affected individual. Not only will receiving two notices about a single breach create confusion and concern among the recipients, it will pose a significant administrative burden and cost for the entity providing the notice. Accordingly, we strongly recommend that the FTC stipulate that the required content listed in proposed Section 318.6 sets forth the *minimum* information that must be included (i.e., the list is not exhaustive) and that the federal breach notice also may include any required elements of the state breach notification laws. A single notice that complies with the content requirements of both the federal and state law is more efficient and sufficiently puts the individual on notice to take the recommended precautions.

ii. Request for clarification regarding contrary state law requirements

The state law conflicts described above may be resolved by permitting PHR vendors and PHR related entities to provide a single notice that includes the requirements of both federal and state law; however, there is at least one circumstance where compliance with the federal law would in fact violate the state notice obligations. Under the Massachusetts security breach notification law, the notice to individuals "shall not include the nature of the breach or unauthorized acquisition or use."[13] In direct conflict, proposed Section 318.6(a) requires that the notice to individuals must include "a brief description of how the breach occurred." In circumstances where a PHR vendor or PHR related entity experiences a breach of PHR identifiable health information that includes data deemed "personal information" under the Massachusetts law (e.g., name plus credit card number), it would be impossible for the vendor or related entity to comply with both the Massachusetts and federal laws when notifying the affected individuals. WebMD believes that the Massachusetts requirement not to disclose the nature of the breach is a contrary state requirement that should be preempted by the federal breach notification requirement.

We note that the Proposed Rule does not address preemption; however, Section 13421(a) of ARRA provides that the preemption requirement set forth in the HIPAA statute (Section 1178 of the Social Security Act) applies to Subtitle D of ARRA, which includes the health breach notification requirement for PHR vendors and other related entities. Under this preemption requirement, a federal provision preempts any contrary provision of state law, with certain specified exceptions.[14] WebMD suggests that the FTC to include this preemption

---

[10] Hawaii, Michigan, North Carolina, Vermont and Virginia.

[11] Iowa and Oregon.

[12] Iowa, Maryland, Oregon and Wyoming.

[13] Mass. Gen. Laws c. 93H, § 3 (emphasis added).

[14] *See* 42 U.S.C. § 1320d-7(a). The exceptions include state laws that relate to the privacy of individually identifiable information. *See* 42 U.S.S. § 1320d-7(a)(2)(B). If the state law at issue relates to the privacy of individually identifiable health information, then a different preemption standard applies – a state law provision is not preempted unless it is contrary to a provision of the Privacy Rule promulgated by HHS and is less stringent than the federal provision. *See* Section 264(c)(2) of Pub. L. 104-191 and as a note to 42 U.S.C. § 1320d-2. This standard has proved burdensome for covered

requirement in the final rule and provide guidance as to what constitutes a contrary state breach notification law. This guidance is essential for PHR vendors and PHR related entities that will need to assess their compliance obligations when they are subject to contrary state requirements such as the Massachusetts requirement not to disclose the nature of the breach.

VI. Conclusion

WebMD appreciates this opportunity to provide the FTC with our comments on the proposed Health Breach Notification Rule. We look forward to working with the FTC in developing a federal breach notification rule that adequately protects the privacy and security of individuals' health information and that is feasible and practical for PHR vendors, PHR related entities, and third party service providers. Should you have any questions about our comments or if WebMD can be of any further assistance to the Commission, please contact Robert D. Marotta at 212-624-3700.

Sincerely,

Robert D. Marotta, Esq.
Senior Vice President &
Chief Regulatory Counsel

---

entities to apply to specific provisions of law and caused great uncertainty when assessing state law obligations.