patientprivacyrights

June 1, 2009

Federal Trade Commission
Division of Privacy & Identity Protection
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580

Attention:
Cora Tung Han, Esquire &
Maneesha Mithal, Esquire,

Re: Health Breach Notification Rule: Notice of proposed rulemaking; request for public comment

Dear Ms. Han & Ms. Mithal:

Patient Privacy Rights (PPR) is a national health privacy watchdog, a 501(c)3 nonprofit. Our mission is to ensure Americans control access to their health records. We educate consumers, champion smart policies and hold industry accountable to protect what is most valuable – our health, our families and our reputations. In addition, PPR leads the diverse, multi-partisan Coalition for Patient Privacy that includes over 50 consumer organizations and technology corporations such as the American Conservative Union, American Civil Liberties Union, Family Research Council, American Association for People with Disabilities, Consumers for Health Care Choices, Liberty Coalition, Consumer Action, AIDS Action and Microsoft Corporation.

We appreciate the Federal Trade Commission's (FTC) thoughtful approach to the proposed interim Health Breach Notification Rule and the opportunity to participate in the discussion. Our comments address three key areas where the FTC should be more cautious and explicit in order to ensure that patients' privacy is upheld:

First, we recommend that the Commission more fully enumerate the types of entities that the proposed interim rule will cover. Clearly, health record platforms such as Google Health and Microsoft HealthVault should be included. PPR recommends that personal genomics companies such as 23andMe also be included. Finally, we encourage the Commission to also add online medical reference services and health-related websites such as WebMD to the list of personal health record (PHR)-related entities subject to the interim rule.

Second, we recommend that the FTC give additional guidance to the distinction between accessing and acquiring, and require entities to support determinations that

no acquisition occurred. Specifically, the FTC should require an entity to determine whether an unauthorized access led to an acquisition by recreating the landing screen. We also recommend requiring that entities keep logs of all investigations for a period of [7] years, particularly in cases where the entity determines there was no unauthorized acquisition. Moreover, the FTC should clarify that any time personal health information is published online, it has been "acquired" for purposes of the rule, given the wide potential exposure and difficulty associated with ever fully securing such data.

Finally, we recommend that the Commission reconsider its position that de-identified data may be excluded from the proposed interim rule in all instances, ie create a new safe harbor. The intent of Congress in the ARRA was not to create new safe harbors, but to protect the privacy of Americans' sensitive health information. There is often a "reasonable basis to believe that [de-identified] information can be used to identify [an] individual," because it is extremely difficult to fully de-identify or anonymize health data. Health data accumulated over time is nearly impossible to de-identify or anonymize. Therefore, we recommend that the FTC include de-identified data within the category of unsecured PHR identifiable health information.

Patients' most sensitive information on earth, their health information, must be treated with the utmost care, caution and concern. We submit these comments in order to help the FTC achieve the important goal of protecting patients and consumers.

Scope

PPR is encouraged by the expansive scope of the proposed interim rule; such scope is necessary to close widening gaps of privacy protection in an increasingly digital environment. Online services that store, aggregate, and analyze patient information have proliferated in recent years. These services can be very valuable to patients as they travel between providers or make decisions about their health. However, given the sensitivity of the information in which these entities deal, there is also great cause for concern and a corresponding need for regulation.

The Commission clearly means to include certain services that store and organized patient health information like Microsoft HealthVault and Google Health within the scope of this rule. These services fall squarely within the definition of PHR related entities and/or vendors of PHR. According to 16 CFR 318.2(f)(3) (proposed), a PHR related entity … "accesses information in a personal health record or sends information to a personal health record." A personal health record is further defined by subsection (d) as: "[A]n electronic record of PHR 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." Also covered by the proposed rule are PHR vendors, which "offer[] or maintain[] a personal health record."

The entire purpose of services such as Google Health and Microsoft HealthVault are to access, send, maintain, manage, share, and control individual's personal health records. These entities purport to "Organize your health information all in one place," "Gather your medical records from doctors, hospitals, and pharmacies," and "Share your information securely with a family member, doctors or caregivers."[1] The Commission clarified that "[e]xamples of entities that could fall within this category include a web-based application that helps consumers manage medications [and] a website offering an online personalized health checklist . . ." Services such as Microsoft HealthVault offer exactly these features.[2] However, to avoid any confusion, the Commission should expressly state that companies providing such services including but not limited to Microsoft HealthVault and Google Health, must comply with the proposed interim rule.

Online services are not limited, however, to the organization and sharing of personal health records. Personal genomics companies such as 23andMe, Navigenics, Knome, and deCODE offer individual genetic testing that can provide customers with novel health services—from determining the likelihood of contracting diabetes, to identifying ancestral roots. Such companies rely on (HIPAA-compliant) labs to analyze patient DNA, which they receive directly, analyze, and store online for access by the patient.

A patient whose genetic information is leaked, stolen, or disclosed could clearly suffer harm as great as that associated with any other PHR health data, as recognized by the various state and federal laws around genetic privacy. The Commission should accordingly determine that personal genomics companies constitute PHR related entities insofar as they "access[] information in a personal health record" or "offer[] or maintain[] a personal health record."

Finally, entities that function as elaborate online medical references and health-related websites that routinely handle individually identifiable health information as defined under the Social Security Act should also be incorporated into the proposed interim rule. WebMD, for instance, offers a survey to determine health risks associated with cholesterol that includes questions regarding a patient's previous diagnoses.[3] Information submitted on WebMD may be associated with an IP address, cookie, web beacon, or other unique identifier reasonably capable of being associated with a patient.[4] Moreover, WebMD invites users to sign in using personally identifiable information for a more personalized experience. We recommend the Commission explicitly designate that entities such as health-related websites and online medical reference services also constitute PHR related entities or vendors and fall under the interim rule.

---

[1] *See* https://www.google.com/health.
[2] *See, .e.g*, "HealthVault In Action," Microsoft HealthVault Promotional Video, available at http://www.healthvault.com/media/HealthVaultInAction.asx (last accessed May 28, 2009).
[3] *See* http://www.webmd.com/cholesterol-management/cholesterol-health-check/default.htm.
[4] *See* http://www.webmd.com/about-webmd-policies/about-privacy-policy?ss=ftr#part3.

Access vs. Acquire

We applaud the FTC's thoughtful analysis with regard to accessing information and acquiring information. PPR strongly supports the FTC's addition to the definition of a breach of security that presumes unauthorized acquisition unless there is reliable evidence showing there has not been, or could not reasonably have been any such unauthorized acquisition. To enforce this valuable rule, we suggest that the FTC require that an entity keep all investigative efforts on file for a period of [7] years—especially in cases where they determine there was no unauthorized acquisition. Absent such a requirement, the Commission will not be in a position to reassess entity representations down the line should patients later discover that they have been harmed by an unauthorized acquisition.

Further, we are concerned that "access" and "acquisition" may not always be separated by a bright line. For instance, the FTC provides the following scenario as an example of an access without acquisition.

> *(3) the employee inadvertently accessed the database, realized that it was not the one he or she intended to view, and logged off without reading, using or disclosing anything.*

This scenario is quite likely, and we highlight it as one in which an entity may find it difficult to prove that the information was not acquired. As the Commission thoughtfully acknowledges, the mere appearance of a patient in a database may constitute sensitive information. But how does one prove whether or not someone has read an item? With health data, simply having knowledge of a condition, medication or procedure can be damaging. Consider for example that the employee is a stalker, abusive partner or ex-spouse. In this instance, it is the individual whose information was breached who may be in the best position to judge whether or not the access was inappropriate, malicious or involved unauthorized acquisition. Simply relying on the employee's role in the company may not be sufficient.

To combat these dangers, the Commission should require an entity to recreate the screen or other medium visible to the employee upon unauthorized access and keep a snapshot of it a period of [7] years. Moreover, the Commission should presume acquisition if the screen was visible to the employee unless it can be proven otherwise.

Finally, another common scenario we have seen is the unauthorized disclosure of PHI online. Multiple instances have been documented that involve a random person conducting an internet search and finding a treasure trove of identifiable health records[5]. Once such information gets out, its potential exposure is world-wide, and it is

[5] Washington Post: Health Insurance Data Mistakenly Put Online: http://www.patientprivacyrights.org/site/News2?page=NewsArticle&id=9365&news_iv_ctrl=-1; Privacy On the Line, WECT Wilmington (NBC)

practically impossible to determine whether and how it has been used. We suggest the FTC clarify in its rule that if information is accessible online in an unauthorized manner, the entity must presume unauthorized acquisition.

De-Identifying Data

The Commission's PHR identifiable health information is appropriately broad. We disagree with the FTC's tentative conclusion, however, that it will not recognize a breach that "involves information that has been 'de-identified' under HHS rules implementing HIPAA." This conclusion stands at tension with the text and spirit of the proposed rule, which specifically includes information "with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." Moreover, Congress' intent in the ARRA was to protect consumers' privacy. We urge the FTC to ensure that existing protections in ARRA are maintained, not undermined by creating more safe harbors.

Re-identification of patient data is all too easy. Experts have noted the ease with which limited data sets (LDS), for instance, can be re-identified. The U.S. Department of Health and Human Services has accordingly imposed a condition upon researchers using LDS that they may not use re-identification techniques. Clearly hackers or others who have acquired PHR in LDS form are under no such obligation, such that unauthorized acquisition of LDS should constitute a breach under the proposed interim rule. Further, Dr. Latanya Sweeney PhD has shown that with the year of birth and 5–digit zip code, .04% of Americans, 12 million people, can be re-identified[6].

In some circumstances, data that is not traceable to individuals can become identifiable when coupled or linked with other public or private information. Thus, for instance, novel techniques have coupled de-identified or "raw" genetic samples with public genealogy records to identify individuals.[7] Given the possibility of re-identifying the de-identified data, the National Institute of Health acknowledged that the current privacy protections for genome wide association studies were not enough and they revised this policy.[8] Experts like Dr. Sweeney have demonstrated methods to provably de-identify health data, so the data is reliable and still protects privacy. This should be the standard for de-identification of data.

---

http://www.patientprivacyrights.org/site/News2?page=NewsArticle&id=9453&news_iv_ctrl=-1; P2P Networks rife with sensitive health care data, researcher warns, Computer World: http://www.patientprivacyrights.org/site/News2?page=NewsArticle&id=9379&news_iv_ctrl=-1

[6] "Strategies for De-identifying Patient Data for Research" by Latanya Sweeney, PhD, http://privacy.cs.cmu.edu/dataprivacy/HIPAA/HIPAAcomments.html

[7] *See, e.g.*, J. Gitschier, et al., *Inferential Genotyping of Y Chromosomes in Latter-Day Saints Founders and Comparison to Utah Samples in the HapMap Project*, 84 The Am. J. of Hum. Genetics 251-258 (2009).

[8] Matt Jones, Forensic Breakthrough Stirs NIH to Close GWAS Data from Public View August 29, 2008, available online at http://www.genomeweb.com/forensic-breakthrough-stirs-nih-close-gwas-data-public-view. "NIH … removed aggregate statistics files of individual GWAS studies, including the Database of Genotypes and Phenotypes (dbGaP), run by the National Center for Biotechnology Information, and the Caner Genetic Markers of Susceptibility database, run by the National Cancer Institute…That data is still available for use by researchers who apply for access to the data and agree to protect its confidentiality using the same approach they do for individual-level study data."

The Commission's recognition that any health information that can be used to identify the individual still counts as PHR identifiable health information is a step in the right direction. The Commission should state expressly that health information that can be coupled with other information counts as PHR identifiable health information for purposes of the proposed interim rule.

Conclusion

While we appreciate the desire to establish reasonable, workable regulations, patients' most sensitive information on earth, their health information, must be treated with the upmost care, caution and concern. In short, when privacy is violated the patient must be informed. **The burden to the data holder cannot trump this important protection for consumers.**

We currently have higher standards and expectations for our financial data than we do for our health data. With a breach of financial records, a consumer faces a significant headache, but ultimately can have their credit and funds restored; this is not the case with health records. A stigmatizing diagnosis, condition or prescription in the wrong hands can cause irreversible damage and discrimination. There is no perfect delete or recover button for Health IT.

PHRs are a virtually unregulated market. PPR urges the FTC to hold the highest standards for breach notification. It is essential that the FTC ensure that breaches are reported in all situations that the average person considers to be a privacy or security breach, so that breach notices apply in a comprehensive way.

Thank you for this important opportunity to provide feedback on this rulemaking process. We look forward to working with the FTC on this and any other critical health privacy matters.

Sincerely,

Ashley Katz
Executive Director