Submitted by Federal eRulemaking Portal

June 1, 2009

Federal Trade Commission (FTC)
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580

16 CFR Part 318 – Proposed Rule

Health Breach Notification Rulemaking
Project No. R911002

Dear Secretary Clark:

iGuard.org is a medication monitoring service designed to provide registered members with timely, personalized drug safety ratings and alerts by electronic mail. Currently, iGuard.org has well over 1 million consumers registered in this program. iGuard.org is not a covered entity (CE) under HIPAA; however, we employ robust administrative and technical measures for the protection of privacy of all individually identifiable data.

Because iGuard.org is an interested party with respect to FTC's Notice of Proposed Rulemaking regarding health breach notification and we are interested in the Secretary's report that is to follow due to our serious commitment to privacy protections, we are pleased to submit the following comments.

Section-by-Section Comments

Proposed 16 CFR Section 318.1: Purpose and scope

The example provided in the proposed rule includes "a web-based application that helps consumers manage medications", which may not involve data directly identifiable to the consumers. Within the limits of the legislative language, we urge the FTC to impose the temporary breach notification requirements of the proposed rule to the range of entities under its jurisdiction in proportion to the extent that they collect, maintain, use or disclose an individual's identifiable health information. We urge that the Secretary and the FTC carefully consider the issue of relative risk to consumers' personal health information in creating the report and recommendations to be delivered to Congress within one year.

Proposed 16 CFR Section 318.2: Definitions

Breach of security – We note that there are differing definitions of breach contained at the American Recovery and Reinvestment Act of 2009 (the "Recovery Act") sections 13407(f) and

13400(1)(A), which should be harmonized. We also observe that Personal Health Record (PHR) identifiable health information is defined broadly, and that PHR vendors, third party service providers and related entities are not provided the kinds of "exceptions" relating to breach specified at section 13400(1)(B). This exceeds the plain language of 13407(f)(1). Further, we find that the Commission has interpreted the legislative language expansively; that is, "unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the 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 reasonably have been, any [emphasis added] unauthorized acquisition of such information." Moreover, the currently accepted standard for breach reporting is that the entity "knows or should have known" that a breach has compromised the security or privacy of information. Instead, the proposed rule places the burden of proof on the entity to show that unauthorized access could not have resulted in acquisition, which greatly expands this currently accepted and reasonable best practice standard.

Personal Health Record related entity

We agree that, because of the nature of the health information that will be accessed or collected in order to perform its function, a "web-based application that helps consumers manage medications" is likely a "related entity". Given the expansive definition of PHR identifiable health information, it may well be that "a website offering an online personalized health checklist" is a related entity. However, we suggest that breach notification requirements be tailored to reflect the actual level of risk to the "security and privacy" of information offered by an individual consumer, especially if such information is "low risk".

Proposed 16 CFR Section 318.3: Breach notification requirement

Proposed section 318.3(b) requires that a third party service provider's notification to a PHR vendor or related entity of a breach shall include "the identification of each individual" whose information "has been, or is reasonably believed to have been acquired during such breach." If the third party provider accesses or uses only as much PHR identifiable health information as required for a given task, such as billing, the "identification" of individuals may not be easy, or even possible. Put another way, if only what HIPAA calls "minimum necessary" information or a "limited data set" has been disclosed to the third party service provider, not only will the PHR vendor or related entity have the burden of breach notification, but it may well have the task of "re-identifying" individuals as well. This re-identification process, undertaken solely for the purpose of sending breach notices about data that poses an extremely low risk, would be costly and burdensome. Moreover, this also would expose the consumers to new and greater risks based on the requisite re-identification process.

Proposed 16 CFR Section 318.5: Methods of notice

Proposed section 318.5(a)(1) requires notification of individuals by first class mail "or, if the individual provides express affirmative consent, by electronic mail." In its analysis, the Commission goes on to explain that "entities may obtain such consent by asking individuals, when they create an account, whether they would prefer… first class mail or e-mail."

iGuard.org provides registered members with timely, personalized drug safety ratings and alerts only by electronic mail. Accordingly, for this purpose, iGuard.org does not collect name, address and other directly identifiable data from the registrants. In addition to collection of minimal information from registrants, other measures that iGuard.org has implemented to ensure privacy protection include encryption for all identifying information, offline (decoupled) storage of indirect identifiers, staff access only to de-identified data, and an automated email distribution system driven by selection of de-identified data.

Under this FTC proposed rule, iGuard.org may be obliged to contact the existing registrants, that is, over 1 million registered individuals by electronic mail, asking (1) whether iGuard.org can send them a notice by electronic mail if there is a breach of health information or (2) whether they wish notification by first class mail. Assuming that the individual responds at all, if that person asks for notification by first class mail, the individual would have to provide his or her name and address to iGuard.org. This would mean that iGuard.org would have to retain directly identifiable data that we would otherwise not need to have. As a result, not only would the risks to consumers' data be heightened, but also the potential liability for iGuard.org would be increased.

This proposed notification approach is contrary to the "Proportionality Principle", which entails a two-step assessment: (i) "whether the means employed by the measure to be evaluated are suitable and reasonably likely to achieve its objectives", and (ii) "the adverse consequences that the measure has on an interest worthy of legal protection and a determination of whether those consequences are justified in view of the importance of the objective pursued".[1] In other words, "[y]ou must not use a steam hammer to crack a nut, if a nutcracker would do."[2]

At proposed section 318.5(a)(1), the Commission states that it "does not regard pre-checked boxes or disclosures that are buried in a privacy policy or terms of service agreement to be sufficient to obtain consumers' express affirmative consent." However, we assert that it is sensible and consistent with the Proportionality Principle for the registrants to be informed in the "Terms and Conditions" of the website that they will receive all communications by electronic mail, including health breach notifications.

Also, proposed section 318.5(a)(4)(i) states that if ten or more individuals cannot be reached by first class mail, e-mail, telephone, or other methods, the PHR vendor or related entity may use two substitute methods of notice, including "through a conspicuous posting for a period of six months on the home page of its website". For online services, this method of substitute notice is preferable to the alternative of a posting in "major print or broadcast media," but the period of six months seems both excessive and arbitrary. Instead, we recommend 30 days or, at most, 60 days.

For reasons of both practicality and consumer protection, iGuard.org recommends that proposed section 318.5(c) be modified to state that the "annual log" of breaches of fewer than 500 individuals be submitted to the FTC in each calendar year in which any breaches occur. The

[1] Christopher Kuner, *Proportionality in European Data Protection Law and Its Importance for Data Processing by Companies*, 7 Privacy & Sec. L. Rep. (BNA) No. 44, at 1615 (Nov. 10, 2008)(citing T. Trimidas, *The General Principles of EU Law* (Oxford University Press 2007) 139).
[2] *Id*. (quoting Lord Diplock in *Regina v. Goldstein* WLR 151, HL (1983)).

proposed rule "starts the clock" from the date of an entity's first breach, which could mean many different entities would submit various starting dates for these annual logs. It would be simpler and of more value to consumers for a PHR vendor or related entity to report that it had "x" number of breaches in the last calendar year. This method of reporting would permit the Commission to aggregate the number of breaches reported by all entities, which would provide useful, reportable metrics for any given year.

Proposed 16 CFR § 318.6: Content of notice

This section is substantively identical to the requirements set forth in the Recovery Act section 13402(f). We point out that the content of the notice required at section 318.6(b) and (c) would vary significantly, depending upon the kind of PHR identifiable health information at issue. That is, a notification from one entity may say, "Your name, address, date of birth, social security number, and health insurance information were acquired by an unauthorized individual, and you should now be aware of possible identity theft, request credit reports, etc." while a notification from another entity may say, "Your over-the-counter medication, age, gender, and ZIP code was accessed by an unauthorized individual, but we do not believe there are steps you need to take to protect yourself from harm at this time." Both "breaches" would require a notice by the PHR vendor or related entity, along with attendant costs. Yet the first notification could provide real value to the individual, while the latter would not provide particularly beneficial information to the consumer. This could be confusing to consumers and lead to their becoming inured to such notifications. Such "equivalence" lacks any real "proportionality" and, therefore, we urge the Commission to be judicious in its enforcement of the final breach notification rule.

* * *

iGuard.org appreciates the opportunity to comment on FTC's Proposed Rule, 16 CFR Part 318. We look forward to working with the Commission as we develop new online and consumer-facing services that will help facilitate clinical and health research. Please do not hesitate to contact iGuard.org for additional information.

Respectfully submitted,

Hugo Stephenson, M.D.
President
iGuard Inc.
66 Witherspoon St #262
Princeton NJ 08542
www.iGuard.org