



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:

Quintiles is a global company, which helps bring new therapies to market by providing innovative, high-quality development, partnerships and commercialization solutions to the pharmaceutical, medical device, and biotechnology industries. Based in North Carolina, Quintiles has over 23,000 employees in offices in 59 countries. Quintiles is neither a covered entity (CE) nor a business associate (BA) under HIPAA. Although Quintiles may collect, transmit, analyze, use and disclose HIPAA protected health information (PHI) in the course of a clinical trial, we do so in accordance with the research participants' informed consent and a HIPAA "Authorization for Research". Moreover, Quintiles has developed a robust global program for the protection of privacy of all individually identifiable data. As we are an interested party in this Notice of Proposed Rulemaking for Health Breach Notification, Quintiles is pleased to submit the following comments.

Section-by-Section Comments

Proposed 16 CFR Section 318.1: Purpose and scope

Within the limits of the legislative language, Quintiles urges 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 ask that the Secretary and the FTC carefully consider the issue of relative risk / scalability in creating the report and recommendations to be delivered to Congress within one year.

Proposed 16 CFR Section 318.2: Definitions

Breach of security – Quintiles notes 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). 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.” This exceeds the clear language of 13407(f)(1). Also, 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 significantly expands the current 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 of minimal 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. In other words, 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 whose disclosure poses 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 of their data.

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.”

For online entities, the only communication between the entity and the individual may well be by electronic mail. Depending on the service offered, the name, address and other directly identifiable data may not be collected at all. Consider, for example, a web-based program that allows consumers to register to receive health-related alerts only by electronic mail. Accordingly, for data protection reasons, it would not be warranted to collect the registrants’ names and addresses for this purpose. Under this FTC proposed rule, the entity may be expected to contact the existing registrants, which may reach into the millions, asking them (1) whether the entity can send them an email if there is a breach of information security 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 the entity. This would pose a new and greater risk to the consumer’s personal data and increase the liability for the entity.

This proposed 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 registrant to be informed in the “Terms and Conditions” of the website that they will receive all communications by electronic mail, including security 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

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)).

to the alternative of a posting in “major print or broadcast media,” but the period of six months seems both arbitrary and excessive. Instead, we recommend 30 days or, at most, 60 days.

For reasons of both practicality and consumer protection, Quintiles suggests 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 proposed rule starts the clock from the date of an entity’s first breach, which could mean many different starting dates for these annual logs from various entities. It would be easier, 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 from all entities and provide useful, reportable metrics for any given year.

Proposed 16 CFR Section 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) will vary significantly, depending upon the kind of PHR identifiable health information at issue. That is, one notice may say, “Your name, address, social security number, date of birth, and health insurance information were acquired by an unauthorized individual, and you should now be aware of potential identity theft, request credit reports, etc.” while another may say, “Your e-mail address, age, and miles jogged over the last week 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” 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 can be confusing to consumers and cause them to become inured of such notifications. Such “equivalence” is disproportionate to the risk. Therefore, we urge the Commission to be judicious in its enforcement of the final breach notification rule.

* * *

Quintiles appreciates the opportunity to provide comment to FTC’s Proposed Rule, 16 CFR Part 318. We look forward to working with the Commission as new online and consumer-facing services are developed that will help facilitate clinical and health research.

Respectfully submitted,

Judith E. Beach, Ph.D., Esq.
Senior Vice President, Senior Associate General
Counsel for Regulatory & Government Affairs, &
Global Chief Privacy Officer
Quintiles
4820 Emperor Blvd
Durham, NC 27703
www.quintiles.com