

Health Care

E-ALERT

April 29, 2009

FTC Seeking Comment on Proposed Breach Notification Rule for Electronic Health Information

The Federal Trade Commission (“FTC” or “Commission”) recently issued a notice of proposed rulemaking¹ relating to the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) provisions of the American Recovery and Reinvestment Act. Section 13407 of the HITECH Act requires vendors of personal health records (“PHR”) and certain other non-HIPAA covered entities to take certain steps to notify affected individuals and the FTC following the discovery of a breach of unsecured PHR identifiable health information. The proposed rule defines “unsecured PHR identifiable health information” to mean “individually identifiable health information,” as defined by HIPAA, that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services (“HHS”).²

FTC will be accepting comment until June 1, 2009. It is anticipated that, once finalized, the proposed rule will apply to all breaches of security discovered on or after September 18, 2009.

I. Scope: FTC-Regulated Entities

The HITECH Act provides the FTC with the authority to issue and enforce temporary³ breach notification requirements applicable to vendors of PHR, PHR related entities⁴, and third party service providers not covered under HIPAA. The FTC proposed rule gives the following examples of PHR related entities that will be subject to the rule:

- A web-based application that helps consumers manage medications.
- A website offering an online personalized health checklist.
- A brick-and-mortar company advertising dietary supplements online.
- Non HIPAA-covered entities that offer products or services through the websites of HIPAA-covered entities that offer individuals PHR.

¹ Health Breach Notification Rule, 74 Fed. Reg. 17914-01 (April 20, 2009) (to be codified at 16 C.F.R. pt. 318).

² According to HHS Guidance, there are currently only two methodologies that render PHR identifiable health information unusable, unreadable, or indecipherable to unauthorized individuals—encryption or destruction. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009. Office of the Secretary. Department of Health and Human Services. April 17, 2009. www.hhs.gov/ocr/privacy.

³ The HITECH Act provides that the FTC has the authority to issue and enforce temporary breach notification rules until Congress enacts new legislation implementing recommendations in a joint HHS/FTC study regarding vendors of PHR and related entities.

⁴ PHR related entities are entities that offer products or services through the website of a vendor of personal health records, entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals personal health records, and entities that are not covered entities and that access information in a personal health record or send information to a personal health record.

COVINGTON

COVINGTON & BURLING LLP

BEIJING

BRUSSELS

LONDON

NEW YORK

SAN DIEGO

SAN FRANCISCO

SILICON VALLEY

WASHINGTON

WWW.COV.COM

- Non-HIPAA covered entities that access or send information to a PHR (e.g., applications through which individuals connect their blood pressure cuffs or other devices, or online weight tracking program that pulls information from a PHR).

HIPAA-covered entities and business associates of HIPAA-covered entities will be subject to HHS, not FTC, breach notification requirements. To the extent that FTC-regulated entities engage in activities as business associates of HIPAA-covered entities, such entities will be subject only to HHS's breach notification requirements. Many of the breach notification requirements are, however, the same for both FTC-regulated entities and HHS-regulated entities.

II. Summary of Notable Provisions

The proposed breach notification rule provides key definitions, timeframes for notification, appropriate methods of notice, and the required content of notices. These provisions are outlined in the HITECH Act and are substantially similar to the requirements relating to breaches of protected health information ("PHI") by HIPAA-covered entities regulated by HHS. Notable provisions in the proposed rule include:

A. Unauthorized Acquisition of Data

The HITECH Act defines a breach of security as "the acquisition of unsecured PHR identifiable health information of an individual in a PHR without the authorization of the individual." In many instances, it will be fairly easy to determine whether unsecured PHR identifiable health information has been acquired without authorization. In other cases, however, there may be unauthorized access to data, but it will be unclear, without further investigation, whether the data has also been acquired. Unauthorized persons may have *access* to information if it is available to them, but the FTC notes that *acquisition* suggests that the information is not only available to unauthorized persons, but in fact has been obtained. Notification of a breach is required only in the event both unauthorized access and acquisition have taken place.

The proposed rule creates a presumption that unauthorized persons have acquired information if they have access to it, but this presumption can be rebutted with reliable evidence. Unauthorized acquisition will be presumed to include unauthorized access without reliable evidence showing otherwise.

B. Maintenance of Reasonable Security Measures

The FTC expects entities that collect and store unsecured PHR identifiable health information to maintain reasonable security measures, including breach detection measures, which should assist them in discovering breaches in a timely manner. If an entity fails to maintain such measures, and thus fails to discover a breach, such failure could constitute a violation of the proposed rule because the entity "reasonably" should have known about the breach. The Commission recognizes, however, that certain breaches may be very difficult to detect, and that an entity with strong breach detection measures may nevertheless fail to discover a breach. In such circumstances, the failure to discover the breach would not constitute a violation of the proposed rule.

C. Notification of Senior Officials

In the event of a breach, the proposed rule requires third party service providers to provide notice to a senior official of the vendor or PHR related entity and to obtain acknowledgment from such official that he or she received the notice. The FTC states that the purpose of this requirement, not present in the HITECH Act, is to avoid the situation in

which lower-level employees of two entities might have discussions about a breach that never reach senior management and to avoid the problem of lost e-mails or voicemails.

D. Content of Notice

The proposed rule provides that e-mail notifications of a breach must not include a request for personal or financial information (in order to avoid phishing concerns) and must identify steps that individuals should take to protect themselves from potential harm.

III. Opportunity for Comment

The FTC is seeking comment on the proposed rule. In particular, the Commission seeks comment on the scope of the proposed rule—the nature of entities to which its proposed rule would apply; the particular products and services they offer; the extent to which vendors of PHR, PHR related entities, and third party service providers may be HIPAA-covered entities or business associates of HIPAA-covered entities; whether some vendors of PHR may have a dual role as a business associate of a HIPAA-covered entity and a direct provider of PHR to the public; and circumstances in which such a dual role might lead to consumers' receiving multiple breach notices or receiving breach notices from an unexpected entity, and whether and how the rule should address such circumstances.

FTC will be accepting comments on its proposed rule until June 1, 2009. Publication of a final rule is expected by August 16, 2009.

If you have any questions concerning the material discussed in this client alert, please contact the following Covington attorneys:

Anna Kraus	202.662.5320	akraus@cov.com
Scott Danzis	202.662.5209	sdanzis@cov.com
Noellyn Davies	202.662.5681	ndavies@cov.com

.....
This information is not intended as legal advice, which may often turn on specific facts. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP is one of the world's preeminent law firms known for handling sensitive and important client matters. This promotional communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts. Covington & Burling LLP is located at 1201 Pennsylvania Avenue, NW, Washington DC, 20004-2401.

© 2009 Covington & Burling LLP. All rights reserved.