Thomas D. Bixby
Law Office LLC
Legal Advice for Health Plans

HEALTH LAW ALERT
April 20, 2009

FTC Proposes Data Breach Rule for Personal Health Records

Proposed Rule Affects Entities Not Subject to HIPAA

Today, the Federal Trade Commission (FTC) proposed a rule to address the unauthorized acquisition of information maintained in personal health record systems sponsored by entities not subject to the HIPAA Privacy Rule, such as Google and Microsoft. *See* 74 *Federal Register* 17914 (Apr. 20, 2009). The proposed rule, which would become a new Part 318 of Code of Federal Regulations Title 16 ("Proposed Rule"), is required by the American Recovery and Reinvestment Act of 2009 ("ARRA"). The Proposed Rule would apply to sponsors of personal health record systems that are not subject to HIPAA and to entities that access information in or provide information to such systems. The Proposed Rule would also apply to entities that offer products and services through the website of any entity—including an entity subject to HIPAA—that offers personal health records.

Entities subject to the Proposed Rule would be required to provide notice of a breach of "unsecured" information discovered on or after September 18, 2009 to (a) individuals affected by the breach, (b) the FTC, and, in cases affecting more than 500 individuals, (c) the media. The FTC requests comments on the Proposed Rule by June 1, 2009. The Proposed Rule would sunset on the effective date of rules implementing future legislation on the subject.

Entities Subject to Proposed Rule

ARRA divides responsibility for regulating entities that offer or maintain personal health records (PHRs) between the Department of Health and Human Services (HHS) and the FTC. Generally, HHS is responsible for regulating PHR data breaches with respect to PHRs sponsored by entities subject to HIPAA and their business associates, whereas the FTC is responsible for regulating PHR data breaches with respect to PHRs sponsored by other entities. Covered entities should nevertheless take note of the FTC's Proposed Rule because ARRA's PHR data breach provisions for HIPAA and non-HIPAA entities are virtually identical and "the FTC is consulting with HHS to harmonize its proposed rule with HHS' proposed rule."

The FTC's Proposed Rule would exclude from the entities it regulates (a) HIPAA covered entities, such as health insurers, and (b) entities while acting in the capacity of business associates to covered entities. The Proposed Rule would apply to other PHR "vendors"—entities that offer or maintain personal health records. Thus, the Proposed Rule would apply to Google, Microsoft, and others that offer PHRs but are not subject to HIPAA (PHR Vendors).

The Proposed Rule would apply to "PHR Related Entities," which are (a) entities that access information in or provide information to a PHR and (b) entities that offer products or services through a PHR vendor's website. This latter category of PHR Related Entity includes an entity that

offers products or services through the website of a HIPAA covered entity that sponsors a PHR. HIPAA covered entities themselves (and their business associates) are excluded from the definition of PHR Related Entity. Third-party service providers—entities that provide services to PHR Vendors or PHR Related Entities—would also be subject to the Proposed Rule.

Notice Requirements

Breach for Which Notice is Required. PHR Vendors and PHR Related Entities would be required to notify each affected individual and the FTC of a breach involving "unsecured PHR identifiable health information." PHR identifiable health information is "individually identifiable health information," as defined in HIPAA, and includes information provided by or on behalf of the affected individual if there is a reasonable basis to believe the information could be used to identify the individual. The information is "unsecured" unless it is protected by a technology or methodology that HHS specifies in guidance. Until HHS issues guidance, information is "unsecured" unless it is rendered "unusable, unreadable, or indecipherable to unauthorized individuals" using standards developed or endorsed by an American National Standards Institute (ANSI) standards developing organization.

An entity experiences a breach of unsecured PHR identifiable health information when an unauthorized person "acquires" the information. The FTC distinguishes between unauthorized "access" to unsecured PHR identifiable health information and unauthorized "acquisition" of such information. Unauthorized "access" would create a presumption of unauthorized "acquisition" under the Proposed Rule. But, an affected entity would *not* be required to provide notice of the breach if it can rebut this presumption with "reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition." Thus, for example, if a PHR Vendor's employee loses a laptop containing unsecured PHR identifiable health information, but the laptop is returned by a third party, the PHR Vendor would be permitted to determine that no breach took place if it could show through "forensic analysis . . . that files were never opened, altered, transferred, or otherwise compromised," even though the third party had "access" to the information.

A third-party service provider that experiences a breach would be required to notify a "senior official" of the affected PHR Vendor or PHR Related Entity and obtain acknowledgement from the official that the notice was received.

Notice to Individual. An entity required to provide notice to individuals under the Proposed Rule would be obligated to provide the notice "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach." The notice would have to be sent by first class mail, unless the individual had provided "express affirmative consent" to receipt of notices by e-mail. The Proposed Rule requires substitute methods for providing notice when initial attempts to provide notice are unsuccessful. When an entity is unsuccessful with respect to providing notice to 10 or more individuals, the substitute method for providing notice must include either a conspicuous posting on the entity's website or publishing notice in "major print or broadcast media" in areas where affected individuals likely reside.

For breaches that affect 500 or more residents of a state or jurisdiction, the PHR Vendor or PHR Related Entity must provide notice to "prominent media outlets serving [the] State or jurisdiction."

Notice by Third Party Service Provider. A third party service provider would be required to provide notice of a breach to the PHR Vendor or PHR Related Entity it serves "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach."

Notice to the FTC. With respect to breaches involving the unsecured PHR identifiable health information of 500 or more individuals, a PHR Vendor or PHR Related Entity would be required to provide notice to the FTC "as soon as possible and in no case later than five business days following the date of discovery." An entity would be permitted to make a single report to the FTC of all breaches involving fewer than 500 individuals once each year, provided that the report of any incident is made no more than one-year after it occurs. The FTC plans to publish instructions for making such reports on its website.

Contents of Notice. Notices would need to include a brief description of how the breach occurred, the date the breach occurred, the date it was discovered, and a description of the types of information involved in the breach. The entity providing notice would have to provide information on what it is doing to (a) investigate the breach, (b) mitigate losses due to the breach, and (c) protect against future breaches. In addition, the notice would have to contain information about what affected individuals can do to protect themselves from potential harm arising from the breach as well as provide procedures for individuals to ask questions or obtain additional information through a toll-free telephone number, an e-mail address, website, or postal address.

FTC Request for Comments

The FTC requests that interested parties provide comments on the Proposed Rule generally. In addition, the FTC seeks comments on several specific subjects, including whether some entities are in dual roles, maintaining PHRs as the business associate of covered entities and as a PHR Vendor, not subject to HIPAA. The FTC seeks information about how the Proposed Rule should address such circumstances.

* * * * *

For more information, about the FTC's proposed rule, ARRA, or other privacy-related issues, please contact Tom Bixby at (608) 661-4310 or TBixby@tbixbylaw.com.

Thomas D. Bixby Law Office LLC
(608) 661-4310 | www.tbixbylaw.com