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

# *HEALTH LAW ALERT*
## *August 25, 2009*

## FTC Publishes Final Data Breach Rule for Personal Health Records
### Minimal Changes From Proposed Rule

Today, the Federal Trade Commission ("FTC") published its final 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* 42961 (Aug. 25, 2009). The rule is a new Part 318 of Code of Federal Regulations Title 16 ("PHR Data Breach Rule"). Although the Rule goes into effect on September 24, 2009, the FTC will "refrain from bringing an enforcement action for failure to provide the required notifications for breaches that are discovered before February 22, 2010." This is because the FTC "recognizes that entities may need to develop new procedures to comply with [the PHR Data Breach Rule]" and will, therefore, need more time to come into compliance.

The FTC is required to promulgate the rule pursuant to the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), which was signed into law by President Obama in February as part of the American Recovery and Reinvestment Act of 2009. The FTC made limited changes to the final rule, based on comments the agency received on its proposed data breach rule, published in May. (Click here for Health Law Alert on the proposed rule.) The PHR Data Breach Rule will sunset on the effective date of rules implementing future legislation on the subject.

The PHR Data Breach Rule applies to (i) sponsors of personal health record systems that are not subject to HIPAA ("PHR Vendors") and (ii) entities that access information in or provide information to personal health record systems or that offer products and services through the website of any entity that offers personal health records ("PHR Related Entities"). Entities that provide service to PHR Vendors and PHR Related Entities ("Third Party Service Providers") are also subject to the Rule. The PHR Data Breach Rule does not, however, apply to a HIPAA covered entity or to an entity while acting as HIPAA covered entity's business associate. Entities subject to the PHR Data Breach Rule must provide notice of a breach of "unsecured" individually identifiable information to (a) individuals affected by the breach, (b) the FTC, and (c) (in cases affecting 500 or more individuals) the media.

The FTC's PHR Data Breach Rule is written to "harmonize" with the Department of Health and Human Services' ("HHS's") data breach rule affecting HIPAA covered entities and their business associates. Indeed, the FTC stresses that in order to avoid "overlap"

between the two rules and to prevent consumers from receiving multiple notices concerning a single event, "compliance with certain HHS rule requirements shall be deemed compliance with the corresponding provisions of the FTC's rule."

**Changes from Proposed Rule**

In the final PHR Data Breach Rule, the FTC made several changes to reflect comments it received on the proposed rule. Among the changes were:

- **Preemption of State Law.** The FTC added a state law preemption provision to clarify that the PHR Data Breach Rule preempts state data breach (and other) requirements under the HIPAA Administrative Simplification state law preemption standard. Hence, the PHR Data Breach Rule preempts state laws that are "contrary" to the federal requirements, where "a state law is contrary to federal requirements (1) if it would be impossible to comply with both state and federal requirements or (2) if state law 'stands as an obstacle to the accomplishment and execution of the full purposes and objectives' of federal requirements." This standard is not, however, likely to preempt many provisions of state law. Affected parties are likely, therefore, to have to comply with both state and federal breach notification provisions, notwithstanding the preemption provision.

- **Default Notice Provided By E-Mail.** The final PHR Data Breach Rule will permit PHR Vendors and PHR Related Entities to make e-mail notification the default for breach notifications, rather than first class mail. The FTC recognized that "email notice is particularly well-suited to the online relationship between consumers and vendors of personal health records." Nevertheless, a PHR Vendor or PHR Related Entity must give consumers a "clear and conspicuous choice" of receiving breach notification by first class mail. The FTC further cautions that entities that elect to "send breach notices by email should provide guidance to consumers regarding how properly to set up spam filters so that [the consumers] will receive such notices."

- **Notice of Third-Party Service Provider Obligations.** The PHR Data Breach Rule adds a requirement that PHR Vendors and PHR Related Entities notify their service providers of their status under the PHR Data Breach Rule. The FTC indicated this provision was necessary to ensure that "a third party service provider [would be aware] that it is dealing with a vendor of personal health records."

- **Third Party Service Provider Notice To PHR Vendor.** A third-party service provider that experiences a breach may notify "an official designated in a written contract by the [PHR Vendor or PHR Related Entity] to receive such notices," rather than a "senior official," as in the proposed rule. The

Third Party Service Provider must obtain acknowledgement from the official that the notice was received. The FTC cautions that contact persons should be "appropriate decisionmakers with sufficient responsibility and authority to oversee the process of notifying consumers."

- **Notice of Breach to FTC.** The PHR Data Breach Rule requires entities to report each breach of less than 500 individuals to the FTC "no later than 60 calendar days following the end of the calendar year," rather than the proposed rule's one year after the first breach experienced. Entities must make the report on a form published on the FTC's website, which, for security reasons, prohibits the entity from (i) including in the report any "personally identifiable information involved in the breach" and (ii) submitting the form by e-mail. The same form is to be used for breaches involving 500 or more individuals, but the form must be submitted within 10 business days of the security breach.

**Breach Notice Requirements**

**Breach for Which Notice is Required.** PHR Vendors and PHR Related Entities are 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 encrypted, destroyed, or protected by another technology or methodology that HHS specifies in future guidance.

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" creates a presumption of unauthorized "acquisition" under the PHR Data Breach Rule. But an affected entity is *not* 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, 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 may determine that no breach took place if it can show through "forensic analysis . . . that files were never opened, altered, transferred, or otherwise compromised," even though the third party had "access" to the information.

**Notice to Individual.** A PHR Vendor or PHR Related Entity that experiences a breach of security must provide notice to each affected individual "without unreasonable delay and in no case later than 60 calendar days after the discovery of [the] breach." When an entity "finds that [its] contact information for ten or more individuals is insufficient or out of date," it must provide substitute notice "reasonably calculated to reach the individuals

affected by the breach" using either (i) a conspicuous posting on the home page of the entity's website for 90 days or (ii) a notice published in "major print or broadcast media" in areas where affected individuals likely reside. The substitute notice must include a toll-free number through which affected individuals may obtain information for at least 90 days.

**Other Required Notice.** A PHR Vendor or PHR Related Entity must provide notice of a security breach to the FTC, as described above (see last bullet under "Changes from Proposed Rule"). In addition, with respect to 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 must 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 of security."

**Contents of Notice.** Notices must be in plain language and include a brief description of what happened, 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 is to provide information on what it is doing to (a) investigate the breach, (b) mitigate harm caused by the breach, and (c) protect against future breaches. In addition, the notice has 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.

* * * * * * * * * *

For more information, please contact Tom Bixby at (608) 661-4310 or TBixby@tbixbylaw.com

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