FTC Seeks Comments on Proposed Health Breach Notification Rule

April 21, 2009

On Thursday, April 16, 2009, the Federal Trade Commission ("FTC") announced approval of a Federal Register notice seeking comments on a **proposed rule that would require consumer and FTC notification in the event of a breach of electronic health information. Comments are due by June 1, 2009**.

The rulemaking is required under the American Recovery and Reinvestment Act of 2009 ("the Act"). Specifically, the Act requires the Department of Health and Human Services, in consultation with the FTC, to conduct a study and submit a report to Congress on privacy, security, and breach notification requirements for vendors of personal health records and related entities by February 2010. Until Congress enacts new legislation, the FTC is required to issue a temporary rule to enforce the Act and to require such entities to notify individuals of potential breaches of the security of their health information.

The Proposed Rule

Application

The proposed Health Breach Notification Rule ("the Rule") would apply to vendors of personal health records, PHR related entities, and third party service providers, and would give the FTC enforcement over such entities, even though such entities would not necessarily fall within FTC jurisdiction. The Rule would not apply to HIPAA-covered entities or business associates of HIPAA-covered entities. The Rule also would regulate a type of personally identifiable information that most state data breach notification laws do not cover. California is currently the only state whose breach notification law is triggered by a breach of an individual's medical or health insurance information.

Key Definitions

PHR Identifiable Information: Individually identifiable information that is provided by or on behalf of the individual, and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Individually Identifiable Information: As defined in § 1171(6) of the Social Security Act, information that: 1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Personal Health Records: An electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily

for the individual.

Vendor: An entity, other than a HIPAA-covered entity, that offers or maintains a personal health record.

Breach: The **acquisition** of the unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual. If the vendor 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 unauthorized acquisition of the information, notification would not be required.

Unsecured: PHR identifiable information that is not secured by a technology standard that renders the information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

Breach Notification Requirement

If a vendor of personal health records discovers that an individual's unsecured PHR identifiable health information has been subject to unauthorized acquisition, the proposed rule would require the vendor to notify all affected individuals, **as well as the FTC**.

In addition, a third party service provider that discovers a breach of security of unsecured PHR identifiable health information would be required to provide notice to a senior official at the vendor to which it provides services and to receive confirmation that the notice has been received. The notice to the vendor would be required to include the identification of each individual whose PHR identifiable health information was acquired during the breach.

Timeliness of Notification

Under the proposed rule, a breach would be considered "discovered" on the first day it is known. The proposed Rule states that notification by a vendor and a third party service provider would be required to be provided "without unreasonable delay," but sets an outer limit of no "later than 60 calendar days after the discovery" of the breach. The 60-day outer limit would, however, constitute "unreasonable delay" if the entity required to provide notice waited until the 60th day to do so.

Methods of Notice

Consumer Notice: Vendors of PHR identifiable health information would be required to provide notice by first class mail or electronic mail, but then, only if the individual had previously provided "express affirmed consent" to be notified by electronic mail. If the entity providing notice determined that the situation required urgency, it would be permitted to contact the affected individuals by telephone or other means, in addition to first class mail or electronic mail. If ten or more individuals could not be reached, the vendor would be required to post notice on its website home page or user landing page for six months, or in major print or broadcast media.

Media Notice: If more than 500 residents of a State or jurisdiction were affected by a breach, the vendor would be required to provide notice to prominent media outlets in the residents' geographic area.

FTC Notice: In addition to consumer notice, vendors would be required under the proposed rule to

notify the FTC following the discovery of a breach. If the breach involved more than 500 individuals, that notification would be required to be provided in no less than five business days following discovery.

Content of Notice

Notice to the affected individuals would have to include:

- a brief description of how the breach occurred, including the date and discovery of the breach, if known;
- a description of the types of unsecured PHR identifiable health information involved in the breach;
- steps the individuals should take to protect themselves from potential harm resulting from the breach;
- a brief description of what the entity is doing to investigate the breach, mitigate losses, and protect against further breaches; and
- contact procedures for individuals to ask questions or learn additional information, which would have to include a toll-free telephone number, an e-mail address, website, or postal address.

Enforcement & Effective Date

Violation of the proposed Rule would be an unfair and deceptive act under § 18(a)(1)(B) of the FTC Act and would be subject to civil penalties. The Rule would apply to breaches discovered on or after September 18, 2009, unless new legislation is enacted.

Request For Comment

The FTC is seeking comment on:

- the nature of entities to which the proposed rule would apply;
- the particular products and services they offer;
- the extent to which vendors of personal health records, PHR related entities, and third party service providers may be HIPAA-covered entities or business associates of HIPAA-covered entities;
- whether some vendors of personal health records may have a dual role as a business associate of a HIPAA-covered entity and a direct provider of personal health records 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.

Kelley Drye & Warren LLP

Kelley Drye & Warren's Privacy and Information Security practice is a leader in advising clients on

privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.