PUBLICATION

FTC Issues Final Health Breach Notification Rule on the Heels of HHS's HIPAA Breach Notification Rule

October 20, 2009

On August 25, 2009, the Federal Trade Commission (FTC) issued its final health breach notification rule. It was effective September 24, 2009; however, the FTC will refrain from enforcement action for breaches discovered before February 22, 2010. The rule requires vendors of personal health records (PHRs) and related PHR entities to notify individuals when the security of their unsecured, individually identifiable health information has been breached. A third-party service provider of PHR vendors that experiences a breach must also notify its vendor or related entity of a breach. In addition to notifying the individual whose information has been breached, these entities must notify the FTC and, in some cases, the media. A violation of these new breach notice requirements is considered an unfair or deceptive act or practice in violation of a regulation under 15 U.S.C. 57a(a)(1)(B) of the Federal Trade Commission Act.

The FTC rule was issued on the heels of the U.S. Department of Health & Human Services (HHS) interim breach notification rule, which applies to covered entities and their business associates.

FTC Rule Has Broad Application

Interestingly, the FTC rule casts a broad net, applying to entities that in the past have not necessarily been directly regulated for their use, storage or retention of health information. Entities such as non-profits (e.g., educational institutions, charities and 501(c)(3) entities) that are normally not within the FTC's traditional jurisdiction are now subject to this breach notice regulation. Third-party vendors subject to the rule will include, among others, entities that provide billing, debt collection or data storage services to PHR vendors or related entities. Foreign entities that have U.S. customers must also comply with this rule if a breach involves U.S. citizens or residents.

The Notice

The rule contains specific requirements regarding the timing of notice, methods of notice and content of the breach notice. Generally, written notice of breach is required without "unreasonable delay and in no case later than 60 calendar days after discovery of the breach." Like the HIPAA rule, it similarly defines "unsecured" and requires special notice to the media in certain circumstances.

The FTC must also be notified. The agency has developed and posted a form for providing that notice on its website and may in a separate federal register notice seek comments on the form and modify it in the future.

What Information is Covered?

The FTC rule applies to a personal health record in electronic form and not to paper records. PHR identifiable information includes the fact of having an account with a PHR vendor or related entity where the products offered are associated with a specific health condition. De-identified data will not be considered PHR. Likewise, name and credit card information will not be considered PHR unless the information identifies an individual as a customer of a PHR vendor or related entity associated with a particular health condition. The FTC declined to adopt a blanket statement that limited data sets are not PHR identifiable health information and similarly

declined to state that "redacted, truncated, obfuscated, or otherwise pseudonymized data" is not PHR identifiable health information. However, if the information could not be used to identify an individual, the information is not PHR identifiable information and is not subject to the rule.

Interplay Between HHS and FTC Rules for HIPAA Covered Entities and Business Associates

The rule generally will not require HIPAA covered entities to report breaches under this rule and therefore also will not apply to business associates of HIPAA covered entities. However, the rule outlines the circumstances when HIPAA covered entities that perform different roles will have to report breaches under both the FTC and HHS rules. Under certain circumstances, compliance with the HHS rule requirements will be deemed compliance with the corresponding provisions of the FTC rule; however, the entity will still have to report the breach to the FTC.

A HIPAA covered entity must also comply with the FTC rule when it creates PHR in a personal capacity and not as a covered entity. (Note: physicians are specifically excluded from the FTC rule unless they provide PHR not as part of their physician practice but in their personal capacity such as in a business enterprise.) The FTC rule will not apply when a HIPAA covered entity offers PHR to its employees. However, when business associates of HIPAA covered entities offer PHR through a HIPAA covered entity or to the public, the business associate could be subject to both the HHS and FTC rule. The PHR vendor's direct offering of PHR to the public puts it under the FTC rule. Its offer to HIPAA covered entity individuals under a business associate agreement makes it subject to the HHS rule. Serving dual roles, the PHR vendor must maintain separate customer lists, one for itself and one for the covered entity. However, a single breach notice for a single breach may suffice to comply with both rules. Further, when the vendor of PHR has direct customers of a HIPAA covered entity with the PHR vendor managing the consumer's PHR account, the PHR vendor would be able to comply with one set of rules, those promulgated by HHS. Interestingly, the covered entity may opt to discharge its breach notice obligation if the notice is provided by the PHR vendor. This obligation would have to be spelled out in the vendor contract with the HIPAA covered entity. The PHR vendor must also notify the FTC.

A PHR vendor may be covered under the HHS rule when it creates a PHR for a patient of a covered entity who moves coverage to another covered entity but takes the PHR with him/her. If the PHR vendor is also a business associate with the new covered entity, any breach will be covered under the HHS rule. If the PHR vendor does not have a business associate agreement with the new covered entity then the patient will be treated as a consumer of the PHR vendor, who will be required to issue a breach notice to the individual as a customer of the PHR vendor under the FTC rule. Therefore, relationships may be fluid and change with the circumstances, triggering differing responses and requirements. The PHR vendor must be vigilant of these changes, track its customers and update its customer lists regularly.

Another example of the dual role of a PHR vendor cited by the FTC is when an individual is employed by a company that has a HIPAA covered group health plan. The group health plan is a covered entity that offers PHR to its employees and their spouses through a PHR vendor that is a business associate of the group health plan. The employee avails herself of the PHR. However, her spouse who is separately insured also avails himself of the PHR offer. In this circumstance a breach triggers the HHS rule for the employee but the FTC rule for the spouse since the spouse is considered a customer of the PHR vendor. The HIPAA covered entity by contract may choose to have the PHR vendor send the breach notice to all customers.

In the event of a breach, the FTC rules should be carefully reviewed and compared with the HHS breach notification rule to assure compliance with all applicable laws. Your Baker Donelson attorney may assist in drafting policies and procedures for compliance. For more information, contact him/her or any of the attorneys in our Health or Technology Law groups.