FTC Issues Health Care Notice of Breach Final Rule Under the American Recovery and Reinvestment Act of 2009

The Rule, which applies to breaches discovered on or after September 24, 2009, regulates vendors of personal health records (PHR) and entities that offer third-party applications for personal health records.

On August 25, 2009 the Federal Trade Commission (FTC) published its final rule relating to notification of individuals when their health information is breached. The FTC's rule, the Health Breach Notification Rule, was enacted pursuant to requirements under the American Recovery and Reinvestment Act of 2009 (ARRA). The Rule applies to both vendors of personal health records (PHR) and entities that offer third-party applications for personal health records. The Rule will apply to breaches of security covered by the Rule that are discovered on or after September 24, 2009.

Who Is Subject to the Rule

The FTC has made clear that its Rule applies to foreign and domestic vendors of PHRs, PHR related entities, and third party service providers, irrespective of any jurisdictional tests in the Federal Trade Commission (FTC) Act. However, it does preempt *contrary* state law as specified in Section 13421 of ARRA. A PHR is defined as an electronic record of 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. PHR-related entities are defined as an entity, other than HIPAA-covered entities or their business associates, that i) offers products or services through the website of a vendor of PHRs; ii) offers products or services through the websites of HIPAA-covered entities that offer individuals PHRs; or iii) accesses information in a PHR or sends information to a PHR. It will take some time to sort through the breadth of these definitions.

The Importance of Secured Health Information

Under the Rule, a breach is deemed to occur if there is unauthorized access to "unsecured" PHR identifiable health information of an individual. The FTC cites to the Guidance issued by the Department of Health and Human Serives (HHS) to determine when PHR information is secured and, therefore, would not require notification. On August 19, 2009, HHS issued its updated Guidance specifying the technologies and methodologies that can be used to secure identifiable health information and render it unusable, unreadable, or indecipherable to unauthorized individuals. For electronic health information, the Guidance requires specific encryption processes approved by the National Institute of Standards and Technology for data at rest and data in transit. The Guidance also addresses the necessary secure methods for retention of the key to the encryption. Specific destruction methods are also indicated for media on which health information is stored (both paper and electronic).

If you have any questions about these rules, please contact one of the following, or your Vorys relationship attorney:

Benita A. Kahn
bakahn@vorys.com
614.464.6487

Melissa J. Mitchell
mjmitchell@vorys.com
614.464.6238

Heather J. Enlow
hjenlow@vorys.com
614.464.6466

Timing of the Required Notifications

In the event of a breach, the FTC's Rule requires the vendor of PHRs and PHR-related entities to notify the affected individuals and the FTC. If a service provider to one of these entities has a breach, it must notify the entity, which in turn must notify consumers. The notice must be made within 60 days of "discovery" of the breach, which is defined as the first day it is known or should have been known. The specific means to notify and the content of the notice is also specified in this Rule. The Rule also requires notification of the media within a state if more than 500 individuals in that state are affected. For breaches affecting less than 500 individuals, the notice to the FTC can be recorded in a log and reported annually.

Other Healthcare Notification Requirement

In addition to the FTC Rule and the HHS Guidance, on August 19, 2009 HHS issued its interim final rule as was required under the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HHS regulations apply to covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates and requires notification if there is a breach of "unsecured" protected health information. Click here for more information on the HHS regulations.