U.S. Department of Health and Human Services Issues Final Rules Requiring Breach Notification for Unsecured Protected Health Information

In general, the rules require covered entities to notify individuals, HHS, and, in some cases, the media, if unsecured protected health information is breached.

On August 24, 2009, the U.S. Department of Health and Human Services ("HHS") published its final rule requiring notification when health information is breached. These rules apply to HIPAA covered entities and their business associates.

In general, the rules require covered entities to notify individuals, HHS, and, in some cases, the media, if unsecured protected health information ("PHI") is breached. Notification to the individual is required no matter how many records have been breached. Business associates are required to notify a covered entity if unsecured PHI under the control of the business associate is breached.

The notification must be made within 60 days of when the breach was, or reasonably should have been, discovered by the covered entity or the business associate. The knowledge of any employee, officer or agent (except for the person who caused the breach) is imputed to the covered entity for purposes of "discovering" the breach. Notification may be delayed so as not to impede a law enforcement investigation or cause damage to national security.

These rules apply for a breach of unsecured PHI that is discovered on, or after September 23, 2009. However, HHS will not impose sanctions for failure to provide the required notification of breaches discovered between September 23, 2009 and February 21, 2010.

Key Concepts

Breach means the acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of the PHI. A breach compromises the security or privacy of the PHI when it poses a significant risk of financial, reputational, or other harm to the individual.

Breaches of health information maintained in limited data sets (from which zip codes and dates of birth have been removed in addition to the elements listed below) and de-identified information do not require notification. Limited data sets have been specified by HHS as data that **does not** include: names; postal address information; telephone numbers; fax numbers; email addresses; SSNs; medical record numbers; health plan beneficiary numbers; account numbers; certificate/ license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; URL's; IP address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

Unsecured PHI means PHI in any form or medium, including electronic, paper or oral form that is not secured by a technology standard that renders it unusable, unreadable or indecipherable to unauthorized individuals. At the same time HHS issued its interim final rule, it also issued updated Guidance on what renders PHI unusable, unreadable or indecipherable. The Guidance makes clear that the only way to secure PHI maintained in paper form is to destroy it.

For further information or assistance in developing an incident response plan, please contact your Vorys attorney or:

Melissa J. Mitchell
mjmitchell@vorys.com
614.464.6238

It also provides the standards necessary to protect electronic data when in transit and at rest. In this regard, the Guidance specifies that the PHI must be protected by using standards created by the National Institute of Standards and Technology ("NIST") as the only means to assert the electronic data was secured. 800-111, Guide to Storage Encryption Technologies for End User Devices (for data "at rest"); 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs or 800-113, Guide to SSL VPNs (for data "in motion").

Finally, once the electronic PHI has served its purpose, it will meet the definition of "secured" under this regulation only if it is destroyed in accordance with NIST standards on destruction. (NIST Special Publication 800-88, Guidelines for Media Sanitation).

Related Federal Trade Commission Rules

On August 25, 2009, the Federal Trade Commission ("FTC") published its final rule governing the notification of breaches of health information to consumers by vendors of personal health records and online applications that interact with these kinds of records. In general, personal health records are online repositories of health information that individuals can create to track their medical visits, prescription information and other sensitive health information. The rule contains specific requirements governing the timing, method and contents of the breach notice to consumers. Click here for more information on the FTC rules.

This client alert is for general information purposes and should not be regarded as legal advice.