More Changes for Health Plans: Mandatory Notices of Breaches of Protected Health Information

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

Linda R. Mendel
lrmendel@vorys.com
614.464.8218

Jolie N. Havens
jnhavens@vorys.com
614.464.5429

Amy M.S. Swank
aswank@vorys.com
614.464.6461

The American Recovery and Reinvestment Act of 2009 (ARRA) created the federal government's 65% subsidy of COBRA premiums. ARRA also included a less publicized section – the Health Information Technology for Economic and Clinical Health Act (HITECH) – that is intended to strengthen the protections afforded to individuals' health information under the current HIPAA privacy and security rules.

The HIPAA privacy and security rules govern the use and disclosure of health information by covered entities (generally, health care providers and health plans). If your company sponsors a self-insured health plan, you probably became familiar with the HIPAA privacy rules in 2003 or 2004 when your company initially implemented privacy policies and procedures for your health plan. Additional steps would have been taken in 2005 or 2006 to comply with the HIPAA security rules.

HITECH requires that a covered entity notify affected individuals without unreasonable delay (and not later than 60 days) after the discovery of a breach of unsecured protected health information. The following definitions are important in determining your obligation to provide notice:

- "Protected health information" (PHI) is individually identifiable health information created or received by (or on behalf of) a health care provider or health plan.
- A "breach" is the acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA privacy regulations which compromises the security or privacy of the PHI.
- The security or privacy of the PHI is "compromised" when the inappropriate acquisition, access, use or disclosure poses a significant risk of financial, reputational or other harm to the individual. The covered entity has the burden of proof when it decides against notice on the basis that the privacy and security of PHI was not compromised.
- A breach is "discovered" when:
  - the breach is known to the covered entity or its business associate;
  - the breach is known to an employee or agent of the covered entity or business associate, other than the individual who committed the breach; or
  - the covered entity, business associate, employee or agent should have known about the breach.
- PHI is "secured" when it is encrypted in accordance with standards specified by the Department of Health and Human Services (HHS) (available at http://www.hhs.gov/ocr/privacy/) or destroyed. Needless to say, it may be impossible to secure all PHI all of the time.
- A "business associate" is an entity that performs a function involving PHI on behalf of the covered entity. For example, a claims administrator is a business associate of a self-insured health plan.

In the event of a breach of unsecured PHI held by or for your health plan, you will be required to send written notice to each affected individual without unreasonable delay (and not later than 60 days) after the discovery. If there is "imminent danger of misuse," you will also be required to provide notice by other means such as telephone and/or e-mail. In addition:

- If a breach affects more than 500 individuals, you must also notify the HHS and inform prominent media outlets. If a breach affects 500 or fewer individuals, it must be recorded in a log and the log must be submitted to HHS annually.
- If you do not have contact information for 10 or more affected individuals, you must post a notice on the health plan's webpage (if it has a webpage) or put a "conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach are likely to reside."
- If your health plan is insured and your company does not get PHI from the insurer, the insurer may be responsible for notification.

Regulations implementing HITECH's breach notification requirements were published on August 24, 2009 and will go into effect 30 days later, on September 23, 2009. However, HHS will not impose sanctions on the failure to provide the required notification of breaches discovered before February 21, 2010 (within 180 days of publication of the regulations and close to February 17, 2010 when other parts of HITECH go into effect). During this 180-day period, HHS "will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance."

In working on compliance, consider the following action items:

- Your health plan's HIPAA privacy and security policies and procedures should be updated for the breach notification requirements.
- Staff members who access PHI as part of their plan administration duties should receive training on the breach notification requirements.
- To make sure you actually do know about a breach when you should know about a breach, you and your business associates will want to have systems in place to detect breaches.
- If the breach involves unsecured PHI under the control of a business associate, the business associate will need to notify the covered entity of the breach and identify all affected individuals. You and your business associates will want to work out the timing and process.

HITECH increased the penalties for violations of the HIPAA privacy and security rules effective February 17, 2009, the date of enactment of ARRA. Penalties are now tiered (ranging from $100 to $1.5 million), based on the knowledge and intent of the violator. Other parts of HITECH go into effect February 17, 2010 and guidance on those parts is expected from HHS. Of particular relevance to self-insured health plans is that business associates become subject to additional duties on February 17, 2010 and those duties will need to be addressed in business associate agreements.

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