New Federal Notice Requirements for the Breach of Unsecured Protected Health Information

In February of this year, the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") was passed as part of the American Recovery and Reinvestment Act of 2009. The HITECH Act contains the first significant changes to HIPAA since its enactment in 1996.

The HITECH Act will require HIPAA "covered entities," such as employer health plans, to revise their HIPAA notices and privacy and security policies and procedures and amend their agreements with business associates, by February 2010.

More immediately, new regulations just issued by the U.S. Department of Health and Human Services ("HHS") take effect on September 23, 2009, and require HIPAA covered entities to provide notice to health plan participants, the Secretary of HHS and in some cases, the media, of a breach of a health plan participant's unsecured protected health information ("Unsecured PHI"). The new federal regulations were published in the Federal Register on August 24, 2009 ("Regulations") and impose requirements on both covered entities and business associates.

Unsecured PHI. The notice required by the Regulations applies only to breaches of Unsecured PHI. Unsecured PHI means PHI that is not secured by a technology standard that renders the PHI unusable, unreadable or indecipherable to unauthorized individuals. According to HHS guidance published on April 27, 2009, encryption and destruction are the only acceptable methods for rendering PHI unusable, unreadable or indecipherable. Unsecured PHI under the federal law includes PHI in any medium, not just electronic data.

Breach. The Regulations define a breach as the acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA privacy rules that compromises the security or privacy of such PHI. The regulations contain certain exceptions to the definition of breach. In the event of a possible breach that does not meet an exception, a covered entity or business associate will need to conduct a risk assessment to determine whether there is a significant risk of financial, reputational, or other harm to the health plan participant. If the covered entity or business associate determines that there is no such significant risk, and therefore no breach, documentation supporting this determination must be maintained because the covered entity or business associate has the burden of proving that there was no breach.

Notice to Plan Participants. If a breach of a health plan participant's Unsecured PHI has occurred, the Regulations require covered entities to notify the participant without unreasonable delay and in no case later than 60 calendar days after discovery of the

breach. A breach is deemed discovered on the first day that it is known, or should have been known by reasonable due diligence, to the covered entity or its business associate. The Regulations also require a business associate to inform a covered entity of any breach it discovers without unreasonable delay and in no case later than 60 calendar days after its discovery. All notices required by the Regulations are subject to a law enforcement delay if the notice would impede a criminal investigation or damage national security. Notices must contain specific elements, such as the type of PHI involved and the steps the covered entity is taking to investigate the breach, mitigate harm and protect against further breaches.

Notice to HHS. If a breach involves 500 or more health plan participants, the covered entity must provide notice of the breach to HHS contemporaneously with the notice it is required to provide to the individual health plan participants. If the breach involves less than 500 participants, the covered entity must maintain a log or similar documentation of each breach and submit the log or documentation to HHS no later than 60 days after the end of each calendar year. For 2009, HHS will require this log or documentation only for breaches that occur on or after September 23, 2009. HHS will provide guidance regarding what information must be included in the log or documentation.

Notice to Media. If a breach involves more than 500 health plan participants, a covered entity also is required to notify prominent media outlets serving the state or jurisdiction where the participants reside without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. Even in cases requiring notice to the media, the covered entity is still required to provide individual notice to the health plan participants affected by the breach.

Implications for Covered Health Plans. Because the Regulations take effect on September 23, 2009, it is important to take action to comply with the new regulations as soon as possible. Covered health plans should determine whether they possess Unsecured PHI and begin to develop policies and procedures for a reasonable breach notice system. Authorized employees with access to health plan PHI must be trained on how to recognize a breach and on the appropriate steps to take if the employee discovers a breach. Business associates must also assure that they have reasonable systems in place to detect breaches and provide notice of any breaches to the applicable covered entity.

Future Regulations. These Regulations are one of several pieces of regulatory guidance HHS is required to issue under the HITECH Act. Please contact one of the attorneys in our Employee Benefits Practice Group if you have any questions about the Regulations or the HITECH Act or would like our assistance in updating your covered health plans' existing HIPAA privacy and security policies.

Employee Benefits Attorneys

Cathryn Conrad	View Resume	cconrad@thompsoncoburn.com
Paul Griesemer	View Resume	pgriesemer@thompsoncoburn.com

Leigh Gutting	View Resume	lgutting@thompsoncoburn.com
Lori Jones	View Resume	ljones@thompsoncoburn.com
Michael Lane	View Resume	mlane@thompsoncoburn.com
Ruth Streit	View Resume	rstreit@thompsoncoburn.com
Patricia Winchell	View Resume	pwinchell@thompsoncoburn.com

For a print version of this Client Alert, click here.
