MURPHY HESSE TOOMEY & LEHANE LLP

Attorneys at Law

Client Advisory
September 2009

Stimulus Bill and HHS Regulations Make Sweeping Changes to HIPAA Breach Rules:

HIPAA Breach Notification Rules Changes Effective September 23

The American Recovery and Reinvestment Act of 2009 ("ARRA"), also known as the Stimulus Bill made important changes to the Health Insurance Portability and Accountability Act ("HIPAA") that affect both covered entities and business associates. On August 24, 2009, the Department of Health and Human Services ("HHS") released final regulations addressing ARRA changes to breach notification requirements. These new regulations will require training for employees who handle protected health information ("PHI"), as well as changes to policies, procedures and business associate agreements.

Prior to the new law, business associates were not directly covered by the HIPAA security and privacy rules. Generally, business associates were held to HIPAA standards through a contractual agreement called a business associate agreement. A covered entity, such as a health plan or health care provider, was required to enter into a business associate agreement with each entity with which it contracted that would have access to PHI. With the ARRA changes, business associates are directly covered under the HIPPA rules. Effective in February 2010 for the most part, business associates will be subject to federal penalties for violation of the privacy and security rules, rather than just breach of contract penalties for violation of a business associate agreement. However, the effective date for the breach notification rules, which apply to business associates as well as covered entities, is September 23.

The new regulations require covered entities to notify individuals when there has been a breach of their PHI. Further, in certain situations, covered entities will have to notify media and HHS when a breach occurs. Business associates will be required to notify covered entities if the business associate has had a breach. The regulations provide a new definition of the term "breach", stating that breach means "the acquisition, access, use, or disclosure of protected health information" in a way not permitted under the regulations "which compromises the security or privacy of the protected health information." Compromises the security or privacy of the PHI means "poses a significant risk or financial, reputational, or other harm to the individual."

Phone (617) 479-5000 Fax (617) 479-6469
www.mhtl.com

Client Advisory
September 2009

These definitions provide for the covered entity and business associate to make a judgment as to how significant the risk is prior to providing any notification. If the entity does not believe there is a significant risk of harm to the individual, it need not make any notification. However, this belief must be reasonable and the entity must be able to document its risk assessment procedure.

Once a breach is discovered the covered entity must provide written notification of the breach the individual without unreasonable delay and at least within 60 days of discovery. Notices are to be sent to the individual's last known address, but if the entity has insufficient or out of date contact information, it may be required to make the notification either through the media or through conspicuous notice on the entity's website. Business associates who discover a breach must notify the covered entity. Business associate agreements will have to be amended to account for these notification rules. If the breach affects more that 500 individuals, the covered entity will have to notify prominent media outlets in the state or jurisdiction. In addition, breaches affecting more than 500 individuals must be reported to HHS immediately. Covered entities must keep a record of smaller breaches and report these to HHS at the end of each year.

These new regulations become effective on September 23, 2009. HHS has stated that it will use its discretion and not impose penalties until February 22, 2010, but it is unclear whether violations of the regulations that occur between September 23, 2009 and February 22, 2010 will be penalized at that time. Therefore, it is important that covered entities and business associates come into compliance as soon as possible. This will require training employees on the new regulations and changes to business associate agreements and privacy policies. In making and implementing these changes, covered entities and business associates should consult with their legal counsel.

* * * * * * * * * *

To discuss the legal issues involved in this matter, please contact Katherine A. Hesse, Brian P. Fox or the attorney that handles your account.

Phone (617) 479-5000 Fax (617) 479-6469
www.mhtl.com