MURPHY HESSE TOOMEY & LEHANE LLP

Attorneys at Law

Labor & Employment Alert
February 2013

Final HIPAA Regulations Require Action by Covered Entities and Business Associates

For a discussion of these and other issues, please visit the update on our website at www.mhtl.com/law. To receive alerts via email, please contact information@mhtl.com.

On January 25, 2013, the Department of Health and Human Services ("HHS") published final regulations making important changes to requirements under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The final regulations are the result of a rulemaking process that has taken over two years and implement changes made in the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which was enacted as part of the American Recovery and Reinvestment Act of 2009, and in the Genetic Information Nondiscrimination Act of 2008 ("GINA"). The new regulations are effective March 26, 2013, and most entities will have to comply by September 23, 2013.

The new regulations expand the definition of business associate to include any vendor that holds or maintains protected heath information ("PHI"), whether or not the vendor views the PHI, and subcontractors of vendors who are business associates. Business associates are also directly liable for compliance with HIPAA Privacy and Security Rules. These changes will require covered entities and business associates to review current business associate agreements to ensure that they are compliant with the new requirements, even if some changes were already made following the passage of HITECH.

The rules also strengthen the rights of individuals with regard to the use of their own PHI. The use of PHI for marketing and fundraising is restricted under the regulations, and written authorization from the individual is required before selling PHI. Under the new regulations, individuals have a right to receive electronic copies of PHI, additional authorization requirements will be put in place on use of PHI for research, and family members of a deceased individual will have greater access to that individual's PHI. Where an individual pays the full cost of a particular treatment, disclosure of related PHI to health plans is restricted. These changes may require covered entities to modify their HIPAA Privacy Policies.

Changes to breach notification rules replace the more subjective standard for determining when notification is required of the risk of harm to affected individuals with a more objective standard with every improper use or disclosure of PHI being presumed to be a breach requiring

notification unless it can be demonstrated that there is a low probability that PHI was compromised. The likely result of this change is that more breaches of HIPAA privacy will require breach notifications to affected individuals, the government and the media.

A new system of penalties for privacy breaches and other transgressions is also in place under the new regulations. The regulations include a tiered monetary penalty system that could lead to stiff penalties for those who do not comply with the HITECH requirements. One important change is that HHS will no longer have discretion to work to resolve issues without issuing a monetary penalty. Penalties for willful neglect of HIPAA requirements can run from $10,000 to $50,000 per violation. With regard to privacy breaches, each affected individual may be considered a separate breach, and ongoing breaches could be subject to daily penalties. The regulations place a cap of $1.5 million per year on violations of a single requirement.

Finally, the regulations implement changes to the HIPAA Privacy Rule, as required by GINA. Under the changes, health plans are prohibited from using or disclosing genetic information for underwriting purposes. This rule was originally proposed in 2009, and some covered entities may have already taken steps to implement it.

The changes implemented by the new regulations will require changes for most current HIPAA policies and business associate agreements. Covered entities and business associates will want to review their policies and business associate agreements now to ensure that they will be compliant as of September 23, 2013.

* * * * * * * * * *

If you have any questions or concerns with regard to the implementation of the Act, please contact Katherine A. Hesse, Brian P. Fox or the attorney assigned to your account.

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