TUGGLE DUGGINS

ATTORNEYS AT LAW

April 12, 2013

New HIPAA Regulations Affect Employers

On January 17, 2013, the Department of Health and Human Services (ñHHSò) released new regulations under the Health Insurance Portability and Accountability Act (ñHIPAAò). Although the new regulations do not substantially alter the fundamental structure of HIPAA compliance, employers will likely need to make some changes to ensure continued compliance.

The new regulations implement tougher privacy and security provisions for covered entities by lowering the security breach notification standard. In addition to the security breach changes, the new regulations impose additional obligations on business associates. As a result business associate contracts may have to be revised to reflect these new obligations.

Changes to Security Breach Notification Standards

The new regulations establish a lower standard for determining whether an employer is required to notify plan participates of a security breach involving their protected health information. The old standard required notification only if an unauthorized use or disclosure of protected health information ñposed a significant risk of financial, reputational, or other harmò to the individual involved. Under the new standard, the employer is required to notify participants of a security breach following *any* unauthorized disclosure of unencrypted protected health information unless the employer can prove that there is a ñlow probabilityò that the protected health information has been compromised based on a four-part risk assessment.

The risk assessment must consider the following factors:

(1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(2) The unauthorized person who used the information or to whom the disclosure was made;
(3) Whether the protected health information was actually acquired or viewed; and
(4) The extent to which the risk to the protected health information has been disclosed.

If, after considering the factors, the employer determines that there is a low probability that the protected health information has been compromised; the employer must document its risk assessment supporting its decision not to notify participants of the breach.

Changes Affecting Business Associates

The final rule also expands the definition of ñbusiness associateò to include subcontractors that create, receive, maintain, or transmit protected health information in performing activities on behalf of a covered entity. As a result, subcontractors of business associates now must also ensure compliance with HIPAA.

What Employers Should Do

Although the final rule became effective on March 26, 2013, the earliest compliance deadline is September 23, 2013, with many deadlines falling much later to allow employers to comply. There are a few things employers should do between now and September.

Revise Privacy Notices:

Employers will need to issue revised privacy notices. This notice needs to (1) inform the recipients of their right to receive security breach notifications, (2) inform the recipient of HIPAAôs new prohibition on the use of genetic information for underwriting purposes, and (3) inform the recipient that the employer is required to obtain the subjectôs authorization before using protected health information for marketing purposes. Employers who maintain a benefits website for their employees should take note, as they need to post the revised notice by September 23, 2013.

Review Business Associate Agreements

The new rule modifies the minimum required contents of agreements with business associates who receive protected health information from a covered entity. In addition to previous requirements, business associate agreements must now include provisions that require business associates to (1) comply with HIPAAôs Security Rule, (2) report any security breaches to the covered entity, and (3) enter into ñdownstreamò business associate agreements with any subcontractor of the business associate who receives protected health information.

The regulations can be accessed on the Federal Registerôs website at: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Please contact D. Ross Hamilton (336) 271- 5279, Denis Jacobson (336) 271-5242, or Sarah Hayward (336) 271-5256 in the employment law and litigation practice groups if you have any questions concerning your compliance with HIPAA.