HIPAA Goes HITECH Under Economic Stimulus Legislation

By Mary V. Bauman; baumanm@millerjohnson.com; 616.831.1704

Included in the economic stimulus legislation are provisions making important changes to the HIPAA privacy and security rules. The changes are included within the Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery and Reinvestment Act of 2009 (ARRA).

The HITECH changes are generally effective as of Feb. 17, 2010. Key new requirements include the following:

STATUTORY REQUIREMENTS FOR BUSINESS ASSOCIATES

Currently, only covered entities (such as health care providers and health plans) are directly subject to the HIPAA privacy and security rules. Business associates (entities that perform a function on behalf of a covered entity which involves the use or disclosure of protected health information (PHI)) were not previously subject to HIPAA. Rather, their only liability was on a contractual basis to the covered entity pursuant to the business associate agreement. That is changing under HITECH. Beginning next year the HIPAA privacy and security rules will apply to business associates in a similar manner as they apply to covered entities.

NEW BREACH NOTIFICATION RESPONSIBILITIES

Currently, if there is a breach of the privacy or security rules, the covered entity is required to mitigate any harm caused by the breach which may, in certain circumstances, include notification. There is no other affirmative obligation to provide notice of a breach. Under HITECH, covered entities must notify individuals within 60 days after discovery of a breach of unsecured PHI. (Any PHI which is transmitted electronically through encryption and any PHI which is destroyed under rules prescribed by the U.S. Department of Health and Human Services (HHS) is not considered unsecured and it is not subject to the new notification rules, even if compromised.) In addition to notifying individuals, HHS must be notified annually of any breaches. If the breach involves 500 or more individuals, HHS must be notified immediately and HHS will identify the covered entity on its website. Further, the covered entity must notify the media (that’s right—alert the media!), if the covered entity reasonably believes that a breach of unsecured PHI affects more than 500 individuals in a state or jurisdiction. Business associates who discover a breach must

Continued on back page
notify the covered entity who then must notify the affected individuals and HHS, and if necessary, the media.

**INCREASED INDIVIDUAL RIGHTS**

HITECH increases individuals’ rights under HIPAA. For example, individuals will now be able to bar health care providers from disclosing their PHI to a health plan for purposes of payment or health care operations if the individual pays for the health care item or service in full on an out-of-pocket basis. In addition, individuals will now have the right to request and receive their PHI in electronic form if the covered entity maintains the information as an electronic health record (EHR). Further, covered entities maintaining PHI as an EHR must supply requesting individuals an accounting of the uses and disclosures of those records for treatment, payment and health care operations purposes during the prior three years. Previously, individuals did not have the right to request an accounting of the uses and disclosures of their PHI for these routine purposes.

**STRENGTHENED ENFORCEMENT**

HITECH significantly strengthens enforcement of HIPAA. Civil penalties are increased and will now vary depending on whether the breach was innocent, due to reasonable cause, or due to willful neglect. HHS will now be required to investigate violations that are alleged to be due to willful neglect. While there is still no private cause of action for HIPAA violations, HITECH provides a mechanism for individuals to obtain a portion of civil monetary penalties recovered by HHS.

**ACTION PLAN**

What do employers need to do in response? HIPAA privacy and security policies and procedures will need to be updated as well as the individual notice of privacy practices. Further, new business associate agreements will be required as well as additional training of your workforce.

Miller Johnson is offering HIPAA workshops on July 7 and 21 in Grand Rapids and July 14 in Kalamazoo (registration can be done on-line at www.millerjohnson.com). This fall we will be offering a HIPAA compliance kit to provide you with instructions on the new steps which must be taken, along with sample documents.

If you have any questions, please contact any member of the employee benefits practice group.