ARRA Changes HIPAA Privacy and Security

Wednesday, March 04, 2009

Not only did the American Recovery and Reinvestment Act of 2009 (ARRA) significantly modify COBRA administration, it made several major changes to the HIPAA Privacy and Security Rules, mandating that a new set of regulations be issued by the Department of Health and Human Services (HHS).

In what ARRA describes as “improvements” to existing law, covered entities, business associates and other entities will soon be subject to more rigorous standards when it comes to protected health information (PHI). Certainly, many well publicized PHI breaches in recent years – and the general lack of rigorous enforcement – contributed to these changes. ARRA also addresses health information technology (HIT). The HIT and HIPAA provisions are contained in a portion of ARRA called the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

All told, the HITECH Act addresses five major areas in the existing HIPAA regulations, with varying effective dates (please see table below):

- Business associates
- Privacy and security breaches
- Disclosure, sales and accounting of PHI
- Health care operations
- Enforcement

Business Associates
Previously, HIPAA applied only to covered entities, which include health plans and health care providers, and indirectly to business associates, which perform PHI-related functions for them. Covered entities were required to execute a business associate agreement (BAA) to ensure that business associates followed the rules.

Under the HITECH Act, all of the HIPAA rules apply directly to business associates, including penalties. In addition, vendors providing data transmission services related to PHI are now considered business associates and must sign BAAs. These might include health information exchange organizations and personal health record (PHR) vendors.

Privacy and Security Breaches
Previously, there was no requirement to report privacy and security breaches, except from the business associate to the covered entity. Under the HITECH Act, covered entities must notify individuals when their unsecured PHI has been compromised and must maintain a breach log, submitting it annually to HHS. Similar rules apply to PHR vendors. HHS is tasked with defining what “unsecured PHI” means by April 18, 2009.

Individual notifications must occur without unreasonable delay within a maximum of 60 days after the breach is discovered. When individuals cannot be located, a covered entity might have to post a notice on its public website. Large breaches require additional notification. If more than 500 people are affected, the covered entity must notify HHS and local print and broadcast media outlets.

Disclosure, Sales and Accounting of PHI
In the past, various entities have used the broad exceptions to the use and disclosure rules to sell PHI for various health-related purposes. Under the HITECH Act, such activity is prohibited.

Individuals have always had a right to receive a covered entity's accounting of PHI disclosures other than those needed for treatment, payment or health care operations. Under the HITECH Act, the exception does not apply to electronic disclosures made in the past three years. An individual can also direct a health care provider to not disclose PHI with the health plan once the provider has been paid in full. An employee can also request access to PHI in electronic format and have it sent to another person or entity.

Health Care Operations

There was always a blurry line when it came to using PHI for marketing purposes, which required individual authorization. Covered entities sometimes asserted that their use of PHI qualified as "health care operations," which do not require individual authorization. The HITECH Act clamps down on this practice. The communication must specifically qualify as an exception to "marketing," and the covered entity cannot receive any compensation in the process. The law provides an exception where the communication describes only a prescription drug or biologic and payment is reasonable in amount.

Enforcement

Although civil money penalties have been available for several years, HHS never imposed a single penalty, opting instead for resolution agreements and consent orders, which sometimes entailed agreed-upon fines. Previously, audits were within the discretion of HHS. Under the HITECH Act, periodic audits are mandatory. Formal investigations of complaints are also required. Noncompliance due to willful neglect must result in the imposition of a civil money penalty. The Attorney General offices of every state can sue individuals for HIPAA violations. The caps on various penalties have been raised, with the top threshold fixed at $1.5 million.

HHS must issue regulations, within the next three years, to allow individuals to receive a portion of any civil monetary penalty or monetary settlement. This new financial incentive may bolster enforcement activity as HHS gets a lot of help from individuals (and presumably their attorneys).

Print | Back