Stimulus Bill's HIPAA Changes

Insights
5.01.09

(Benefits Update, No. 2, May 2009)

The American Recovery and Reinvestment Act (ARRA), signed by President Obama into law on February 17, 2009, included changes to the health information privacy and security rules under HIPAA, the Health Insurance Portability and Accountability Act of 1996.

ARRA imposes many privacy and security standards directly on business associates, requires new notification requirements for an unauthorized disclosure of protected health information (PHI), expands rights for individuals who are the subject of PHI, increases penalties and grants enforcement authority to states' attorneys general.

The New Rules
Generally, a "business associate" is an entity that provides services to a covered entity (a group health plan), such as claims processing, data analysis, recordkeeping, actuarial services, etc. Now, business associates are directly subject to the technical, physical and administrative provisions in the HIPAA security standards, just like covered entities have been for the last few years. This change requires business associates to complete a security risk analysis, appoint a HIPAA security official and develop written policies and procedures to govern the security of electronic PHI. Business associates are now subject to civil and criminal penalties for violations of HIPAA's privacy and security rules.

ARRA also added a notification requirement that applies to all covered entities and business associates. They must notify individuals of a breach of their "unsecured PHI" within 60 days of discovery of the breach (entities are deemed to have knowledge of a breach if they "should reasonably have known" about it). Notification must be written and sent by first class mail to the individual's last known address, or may be electronic mail if the individual previously consented to electronic notice.

If there is insufficient or out-of-date contact information, covered entities may satisfy the notice requirement with a conspicuous posting on its webpage or a notice in newspapers or broadcast media. This substitute notice must include a toll-free phone number that individuals can call to verify if their PHI was affected. Breaches that affect more than 500 individuals also must be reported to HHS, which will publicize the breach on the HHS website. For breaches that affect fewer than 500 people, covered entities must keep a log to be submitted annually to HHS.

Individuals may request an electronic copy of their PHI if the information is stored electronically, and the copy must be provided at cost. Individuals may restrict disclosures of their PHI to a health plan if the purpose of the disclosure is not related to treatment and the cost of the service has been paid in full. Finally, individuals also may request an accounting of disclosures of their electronic PHI if the disclosures were made for treatment, payment or health care operations.

The New Penalties

ARRA significantly increases civil monetary penalties for HIPAA violations and introduces a tiered penalty structure. Effective February 17, 2009, penalties, which were $100 per violation before ARRA, are now $1,000 per violation if due to "reasonable cause and not to willful neglect" (capped at $100,000 per calendar year), $10,000 for each violation due to "willful neglect" that is corrected (capped at $250,000 per calendar year), and $50,000 for each violation due to "willful neglect" that is not corrected (capped at $1,500,000 per calendar year). Also, criminal penalties may apply to an individual or employee of a covered entity that obtains PHI without an individual's authorization. State attorneys general are now authorized to file suit on behalf of their residents in federal court.

HHS is now required to conduct periodic audits of covered entities and business associates to verify their compliance with HIPAA's privacy and security rules. This means HHS will soon be conducting random audits to ensure that covered entities and business associates have completed all of their required administrative steps (training, plan amendments, employer certifications, policies and procedures, privacy notice, etc.).

A version of this article was reprinted in the June 25, 2009 issue of the San *Francisco Daily Journal*.

Service Focus

Privacy and Cyber