HIPAA Compliance Efforts Should be Revisited

06.26.09

HIPAA Compliance Efforts Should be Revisited

Covered entities and business associates should revisit their compliance efforts under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to address the recent expansion of the HIPAA privacy and security rules. A failure to comply with the expanded rules could subject the covered entity and business associate to civil penalties, the amount of which were significantly increased.

Background

On February 17, 2009, President Obama signed into law, the American Recovery and Reinvestment Act of 2009 ("Act"). On April 17, 2009, the Department of Health and Human Services ("HHS") issued guidance and proposed rules addressing various aspects of the Act. As to privacy and security issues, the Act and HHS pronouncements generally provide, among other items:

Increased Obligations for Business Associates. Prior to the Act, business associates were not directly obligated by HIPAA to comply with the use and disclosure requirements of protected health information ("PHI"); however, business associates were contractually obligated to comply through business associate agreements with covered entities.

Effective February 17, 2010, the Act provides that HIPAA privacy and security rules generally apply to business associates in the same manner as they apply to covered entities. This means that business associates will be subject to the administrative, physical and technical safeguard requirements of the privacy and security rules.

New Breach Notification Requirement. Prior to the Act, a covered entity was not required to notify individuals if there was a data security breach of their PHI unless the covered entity concluded such notification was required to mitigate harm to such individual or was otherwise required under applicable state law

Likely effective September 15, 2009, the Act requires covered entities to notify applicable individuals if their unsecured PHI has been accessed, acquired or disclosed as the result of a breach. And if a business associate discovers the breach, the Act generally requires that the business associate notify the covered entity of the breach and the identity of the individual whose PHI was compromised within 60 days from discovering such breach. Noteworthy is that notice through media outlets is required if the breach involves PHI of more than 500 individuals (the Act also addresses other notice requirements). Also noteworthy is that the Act's breach notification provisions do not preempt more restrictive state security breach notification laws.

Securing PHI. The breach notification requirements only apply to unsecured PHI (i.e., a breach of secured PHI would not trigger the breach notification requirements). On April 17, 2009, HHS issued guidance on the proper methods for securing PHI. The guidance defines secured PHI as that which is "unusable, unreadable, or indecipherable to unauthorized individuals." Under HHS guidance, the two methods for securing PHI include destruction and encryption (the latter of which is defined as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key"). Addressing the encryption requirement, PHI will be deemed secure if the encryption satisfies the standards published by the National Institute for Standards and Technology.
Expands Accounting for Disclosures of PHI. HIPAA requires covered entities to account for disclosures of PHI. Prior to the Act, disclosures made for purposes relating to treatment, payment or health care operations were excepted from this

accounting requirement.

Effective January 1, 2011 or January 1, 2014, the Act requires covered entities to account for disclosures made for treatment, payment and health care operations purposes if such covered entity uses or maintains electronic health records. This new requirement includes disclosures from covered entities to business associates (which prior to the Act were excepted as disclosures relating to health care operations).

Increased Civil Penalties

Currently in effect (excepting "willful neglect" provisions which are not effective until February 2011), the civil penalties for violating the HIPAA privacy rule or security rule are as follows:

Tier	Penalty
Tier 1 – Person unaware of violation:	$100.00 per violation, not to exceed $25,000 for all violations of same requirement in same calendar year
Tier 2 – Violation due to reasonable cause (no willful neglect):	$1,000 per violation, not to exceed $100,000 for all violations of same requirement in same calendar year
Tier 3 – Violation due to willful neglect, corrected within 30 days:	$10,000 per violation, not to exceed $250,000 for all violations of same requirement in same calendar year
Tier 4 – Violation due to willful neglect, not corrected within 30 days:	$50,000 per violation, not to exceed $1.5 million for all violations of same requirement in same calendar year

Additionally, and currently effective, the Act provides a state's attorney general with the ability to bring an enforcement action on behalf of the residents of its state and obtain damages (including and attorney fees).

Action Items

Covered entities and business associates should revisit their HIPAA compliance efforts to minimize their exposure to PHI security and breach notification requirements. This effort would include revising business associate agreements to address their increased obligations under HIPAA, and revising policies and procedures to address breach notification obligations. Additionally, business associates should act now to analyze the full impact of their increased obligations under the Act, which could require substantial compliance efforts.