

## Management Alert

# Stimulus' Expansion of HIPAA Privacy and Security

While most of the buzz surrounding the American Recovery and Reinvestment Act of 2009 (the "Act") is about tax cuts, spending, and even perhaps COBRA subsidies, changes to the privacy and security rules for health plans and providers have quietly snuck in. The Act provides major changes to the privacy and security rules under the Health Insurance Portability and Accountability Act (HIPAA). The Act also provides for increased enforcement and penalties for non-compliance. Highlights of the changes are described below.

### *Business Associates Subject to HIPAA Independently*

Prior to the Act, only covered entities (including health plans and providers) were subject to the requirements of the HIPAA Privacy and Security Rules. Those assisting covered entities, known as business associates, were not directly subject to the Privacy and Security Rules. Instead, the covered entity was required to contract with the business associate to make sure that the health information to which the business associate had access was protected.

Under the Act, the HIPAA privacy and security standards, as well as the civil and criminal penalties for violating those standards, now apply to business associates in the same manner in which they apply to covered entities.

### *Notifications of a Breach*

The HIPAA regulations did not directly require covered entities to notify Health and Human Services (HHS) or individuals of a breach regarding the privacy or security of their protected health information (PHI). Whether notification was to be made was part of the covered entity's analysis of how to mitigate the breach and to adjust procedures to prevent its recurrence.

The Act now requires the covered entity to notify each individual whose unsecured PHI has been compromised (a "breach") and keep a log of such breaches to be submitted annually to HHS. The notification to the individual must be made without unreasonable delay but no later than 60 days following discovery of the breach.

### How to Give Notice

The notification of a breach must be in writing by first class mail, or where a preference is stated, by electronic mail. If the covered entity does not have sufficient contact information then a substitute form of notice is to be provided, which, if more than 10 individuals are involved, may include posting on the covered entity's website site or notice in major print or broadcast media. If a possibility of imminent misuse of the protected health information exists, then notification should be by telephone or other appropriate means.

Further, if the breach involves the data of more than 500 individuals, the covered entity must notify HHS at the time of the discovery as well as “prominent media outlets” in the area. Reported breaches of this magnitude will be posted on the HHS website for public viewing.

The Act clarifies that notification of even unintentional disclosures would be required unless such disclosure is to an individual who is authorized to access health information at the same facility. “Unsecured” PHI generally means information that is not encrypted or secured in such a manner as to make it unreadable to an unauthorized person. However, HHS is to issue guidance on the meaning of “unsecured” by April 18, 2009.

### *Individual Rights*

The Act expands the rights an individual currently has under the HIPAA Privacy Rule. Here are some key changes:

- Currently, individuals have a right to receive an accounting of disclosures of their PHI made by the covered entity over the prior six years, other than disclosures made to carry out treatment, payment, or health care operations of the covered entity. The Act expands this right by providing that the exception for disclosures made to carry out treatment, payment, or health care operations does not apply to disclosures made through an electronic health record. In this case, the individual may receive an accounting of any electronic disclosures made by a covered entity or a business associate during the previous three years.
- The Act now allows an individual to direct a health care provider to not share his or her PHI with his or her health plan if the provider involved has been paid out of pocket in full. Previously, the covered entity could determine whether to comply with such a request for restrictions.
- Currently, the use or disclosure of PHI is limited to—in most cases, but not all—that which is minimally necessary. The Act provides that the covered entity must now limit all of its uses, disclosures, or requests for PHI to that which is minimally necessary or contained in a limited data set.
- The HIPAA Privacy Rule currently allows an individual to request access to his or her PHI. The Act expands that right to allow an individual to request PHI in an electronic format and to direct it to be sent to another designated person or entity.
- Finally, the Act provides a prohibition against covered entities and business associates selling any PHI without the specific authorization of the individual.

### *Enhanced Enforcement Provisions*

Previously, HHS was authorized to conduct audits of HIPAA privacy and security compliance. The Act now mandates such audits be conducted to ensure compliance. The Act also *requires* a formal investigation of complaints, as well as imposition of civil monetary penalties for violations due to willful neglect.

The Act authorizes individual state Attorneys General to bring a civil action against individuals who violate the HIPAA privacy and security standards, in order to enjoin further such violation and seek damages of up to \$100 per violation—capped at \$25,000 for all violations of an identical requirement or prohibition in a calendar year.

### *Effective Date*

For the most part, the provisions are effective February 17, 2009, however, some provisions have a delayed effective date tied to guidance issued from HHS.

### *Considerations & Impact of the Law*

- Covered entities must review and revise their HIPAA privacy and security policies, as well as administrative materials, record retention policies, and training logs to comply with the new provisions.
- Covered entities will need to revise their HIPAA privacy notices to reflect the new provisions.
- Covered entities should review their business associate agreements. Most agreements will need to be modified to reflect the new requirements.
- Business associates must take steps to determine whether they need to adopt HIPAA policies and related materials that reflect their new status as directly subject to HIPAA.
- Covered entities and business associates must properly train any employees who have contact with PHI from the group health plan on the new standards.

*For more information, please contact the Seyfarth attorney with whom you work, or any attorney on our website ([www.seyfarth.com](http://www.seyfarth.com)).*



Breadth. Depth. **Results.**

[www.seyfarth.com](http://www.seyfarth.com)