Foster Garvey

HIPAA Gets 'Stimulated'

Legal Alert
February 5, 2009

Garvey Schubert Barer Legal Update, February 5, 2009.

On February 17, 2009, President Barack Obama signed into law the “Stimulus Bill” formally known as The American Recovery and Reinvestment Act of 2009 [1 MB PDF]. While much of the 1,100 page document has received great attention, the 50 pages amending the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have gone virtually unnoticed. For healthcare providers these 50 pages of amendments represent significant changes in the scope of HIPAA and how it will be enforced.

August 24, 2009 Update: View a copy of new proposed regulations (specifically Department of Health and Human Services, 45 CFR Parts 160 and 164, Breach Notification for Unsecured Protected Health Information; Interim Final Rule.)

This Healthcare Law Alert does not purport to discuss every change to HIPAA brought about by the Stimulus Bill. However, the following areas of HIPAA have all been amended by the Stimulus Bill and should be of substantial concern to healthcare providers:

Privacy and Security Provisions Now Directly Applicable to Business Associates

Notification in the Case of Breach

Disclosures Required to be Limited to Limited Data Sets or Minimum Necessary

Breach Notification Requirements for Vendors of Personal Health Records

“Improved Enforcement”

Federal Preemption of State Law

Privacy and Security Provisions Now Directly Applicable to Business Associates

Business associates under HIPAA are companies or persons hired under contract by a covered entity to perform a function or activity that requires the business associate to review or process protected health information supplied by the covered entity.[1] When HIPAA was first established it placed on covered entities the burden of ensuring that their business associates complied with HIPAA and not disclose protected health information improperly. This was achieved through a contract called a “business associate contract.” Today this contract is more typically referred to as a “business associate agreement.”[2]

The Stimulus Bill fundamentally alters the current law and makes the HIPAA privacy and security requirements applicable to business associates to the same extent that they “are made applicable with respect to covered entities…” The Stimulus Bill also requires that the

HIPAA privacy and security requirements “shall be incorporated into the business associate agreement between the business associate and the covered entity.”

Application of Civil and Criminal Penalties to Business Associates:

The new law states specifically that if a business associate violates applicable standards of the privacy or security rules the appropriate civil and criminal penalties “shall apply to the business associate with respect to such violation in the same manner such [penalties] apply to covered entities” that violate such privacy and security provisions.

Notification in the Case of Breach

HIPAA, as originally passed, does not mandate that a healthcare provider notify an individual if their health care information is improperly disclosed. Instead, individuals must request an accounting of disclosures. 45 C.F.R. §164.528. Many healthcare providers voluntarily report improper disclosures of protected health information to the affected individuals, but that is not required by HIPAA.

The Stimulus Bill significantly changes this. With the passage of this Bill, HIPAA now requires that individuals be notified by the covered entity that improperly discloses or allows access to, or reasonably believes they disclosed or allowed access to, the individual’s unsecured protected health information. “Unsecured protected health information” is defined as “protected health information that is not secured through the use of a technology or methodology specified by the Secretary [of Health and Human Services].”[3] §4402 (h)(1). If the breach is discovered by a business associate, the business associate is only required to notify the covered entity.

All breach notifications must be made “without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity (or business associate) involved in the case of a notification required [of the business associate].” §4402 (d)(1).

Methods of Notification:

If the covered entity knows the address of the individual whose unsecured protected health information has been improperly disclosed the covered entity is to give written notice by first-class mail.

If direct notification by mail is not possible and 10 or more individuals are affected by the breach, the covered entity can make “a conspicuous posting for a period determined by the Secretary on the home page of the Web site of the covered entity involved or notice in major print or broadcast media ... ” The notice for the media or on the home web page must “include a toll-free phone number where an individual can learn whether or not the individual’s unsecured protected health information is possibly included in the breach.”

Breaches Involving 500 or More Individuals:

If the unsecured protected health information of 500 or more individuals occurs, the covered entity must give notice immediately to the Secretary.

Breaches Involving More Than 500 Individuals:

If the unsecured protected health information of more than 500 individuals of a state occurs, notice must be provided to “prominent media outlets” serving the state.

If the unsecured protected health information of more than 500 individuals occurs, the Secretary will identify on its website the covered entity involved with the improper disclosure.

Additional Notification to the Secretary:

If the unsecured protected health information of fewer than 500 individuals occurs, the covered entity may notify the Secretary immediately or may keep a log documenting the breach and annually submit the log to the Secretary.[4]

Content of Notification:

Regardless of the method by which notice is provided to individuals, notice of a breach must include, to the extent possible, the following:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
3. The steps individuals should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Disclosures Required to be Limited to Limited Data Sets or Minimum Necessary

Until the Secretary of HHS issues specific guidance of what constitutes “minimum necessary,” covered entities will be treated as being in compliance with HIPAA if their disclosure of PHI contains only the information that constitutes the “limited data set” as that term is defined in the privacy rules. If information beyond the limited data set is needed the covered entity can still remain in compliance with HIPAA if the additional PHI is the minimum necessary needed to

meet the intended purpose for the use or disclosure of that information.

Breach Notification Requirements for Vendors of Personal Health Records

Vendors of Personal Health Records (PHR) and their third-party service providers were not subject to HIPAA.[5] In order to fill this perceived gap in coverage the Stimulus Bill includes provisions applicable to PHRs requiring them to report security breaches similar to those noted above applicable to covered entities and business associates. The major distinction for PHRs is that breaches of the privacy or security of unsecured PHI requires the PHR to notify the Federal Trade Commission (as opposed to the Secretary of HHS) as well as the affected individuals (if they are citizens or residents of the United States) of the breach.

Failure to comply with these notification requirements concerning breaches of the privacy and security rules applicable to PHRs are deemed to be unfair and deceptive trade practices under the Federal Trade Commission Act.

“Improved Enforcement”

The Stimulus Bill makes a number of significant changes to the HIPAA criminal and civil penalties and how those penalties will be enforced. The Stimulus Bill enforcement section begins by clearing up any confusion about whether the criminal penalties apply to individuals. There has been a debate about whether the penalty provisions apply to individuals or employees of covered entities since individuals working for a covered entity may not fit within the strict definition of a covered entity. Any lingering confusion is cleared up in the new Bill that now provides that the criminal provisions of HIPAA apply to employees and other individuals who use or disclose individually identifiable information obtained or disclosed without authorization if the information is maintained by a covered entity. As used in the Stimulus Bill the term “authorization” appears to mean legal authority as opposed being limited to a formal written authorization.

HIPAA Audits:

The Stimulus Bill continues the Office of Civil Rights (OCR) recent shift towards conducting audits looking for HIPAA violations as opposed to just relying on complaints filed. The Secretary of HHS is now required to provide for periodic audits of covered entities and business associates to ensure compliance with HIPAA. Presumably the Secretary will delegate this audit function to OCR and OCR will continue with its current role of investigating HIPAA complaints.

Willful Neglect:

Within 18 months of the effective date of the Stimulus Bill the Secretary must promulgate regulations that impose a mandatory civil penalty for any HIPAA violation due to “willful neglect.” Further, the Secretary must formally investigate any complaint of a HIPAA violation if a

preliminary investigation of the facts of the complaint indicate a possible violation of HIPAA due to willful neglect.

Distribution of Civil Monetary Penalties Collected:

Any monetary settlements or monetary penalties collected with respect to a violation of the HIPAA privacy or security rules will now be transferred to OCR to be used for purposes of enforcing the HIPAA provisions of the Stimulus Bill and the HIPAA privacy and security rules.

In addition to the above, not later than 18 months after the date of the enactment of the Stimulus Bill, the Comptroller General must submit to the Secretary of HHS recommendations for a methodology under which an individual who is harmed by a HIPAA privacy or security breach may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such HIPAA violation.

The Secretary of HHS has three years from the date of enactment of the Stimulus Bill to adopt regulations based on the above-noted recommendations from the Comptroller General creating a methodology under which an individual who is harmed by a violation of the HIPAA privacy or security regulations the harmed individual may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such HIPAA violation.

Tiered Increase in Amount of Civil Monetary Penalties:

The increased penalties for HIPAA violations or the HIPAA provisions of the Stimulus Bill go into effect immediately. Under the new statutory scheme four “tiers of penalties” are created. Which tier is applicable is determined by weighing the nature and extent of the violation, the nature and extent of harm caused by the violation, whether the violator took steps to correct the violation when discovered, and the state of mind of the violator when they committed the violation. The four tiers are:

Tier A: *State of Mind:* Violation where the violator did not know (and by exercising reasonable diligence would not have known) that they were violating HIPAA. *Penalty:* $100 for each violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.

Tier B: *State of Mind:* Violation due to reasonable cause and not willful neglect. *Penalty:* $1,000 for each violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $100,000.

Tier C: *State of Mind:* Violation due to willful neglect but the violation was corrected. *Penalty:* $10,000 for each violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $250,000.

Tier D: *State of Mind:* Violation due to willful neglect and the violation was not corrected. *Penalty:* $50,000 for each violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.

Enforcement Through State Attorneys General:

The Attorneys General of the various states are now empowered to bring a civil action in federal court on behalf of the residents of their states who have been or who are adversely affected by any person who violates HIPAA or the HIPAA provisions of the Stimulus Bill. The Attorneys General are empowered to seek injunctions to enjoin any further violations or to seek damages calculated in a manner that is consistent with the Tier A damages limitation noted above. If the prosecution is successful, the court may award the State Attorneys General the costs of the action plus a reasonable attorney fees amount.

Prior to bringing an action in federal court, the State Attorneys General, where feasible, must give written notice to the Secretary of HHS of their intent to do so accompanied by a copy of the complaint they intend to file. The Secretary may intervene in the action. The State Attorneys General may not bring an action if the Secretary of HHS has already brought an action.

Federal Preemption of State Law

As with the enactment of the original HIPAA, HIPAA rules apply unless there is a state law that is more restrictive than the HIPAA provisions. Most providers engaged in a HIPAA Preemption Analysis when HIPAA first passed. With the enactment of the Stimulus Bill provisions, healthcare providers would be wise to revisit their HIPAA Preemption Analysis in light of these new HIPAA provisions.

---

[1] For the full definition of a “Business Associate” see 45 C.F.R. §160.103.

[2] The federal government published “Sample Business Associate Contract Provisions.” See, e.g., 67 Fed. Reg. No. 157, pp. 53264-53266 (Aug. 14, 2002).

[3] The Secretary of Health and Human Services is directed by the Bill to issue guidance specifying the technologies and methodologies that render protected health information unusable. The Secretary must issue the initial guidance within 60 days of the enactment of the Stimulus Bill and then update the guidance annually.

[4] Reading these notice requirements together one gets a patchwork of notice requirements:

1. *Breach involves 499 individuals or less:* Covered entity to give written notice by first-class mail to individuals with known addresses. If addresses of 10 or more individuals not known, notice may be given by a conspicuous posting on the covered entities home web page or

give notice in major print or broadcast media including in the notice a toll-free phone number for individuals to call.

2. *Breach involves 500 or more individuals:* Must do same as 1, plus notify the Secretary of Health and Human Services immediately.
3. *Breach involves 501 or more individuals:* Must do same as 1 and 2, plus Secretary of Health and Human Services will post covered entity information on HHS web page.
4. *Breach involves 501 or more individuals from the same state:* Must do same as 1, 2, and 3, plus must provide notice to prominent media outlets serving the state.

[5] "Vendor of Personal Health Records" is defined as an "entity, other than a covered entity, that offers or maintains a personal health record."