EPSTEIN BECKER GREEN | HEALTH CARE & LIFE SCIENCES CLIENT ALERT

Thought Leaders in Health Law®

American Recovery and Reinvestment Act: Overview of Modifications to the HIPAA Privacy and Security Regulations

by Robert Hudock, Esq. CISSP, and Mark Lutes, Esq.

February 17, 2009

This alert provides a brief overview of privacy and security provisions included within The American Recovery and Reinvestment Act of 2009 (H.R. 1, S. 1) (the "Stimulus"). The Stimulus includes funding for health information technology ("HIT") and for comparative effectiveness research. These provisions will be the subject of future alerts. Future alerts will also provide analysis and risk management suggestions related to the changes outlined below.

The Stimulus expands enforcement and the scope of businesses covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security regulations. That is the focus of this alert. The Improved Privacy Provisions and Security Provisions contained within the Stimulus are expected to have a significant impact on a wide range of organizations that deal with, retain, use, and/or create protected health information (PHI). The privacy and security provisions are outlined in Table 1 (below). The provisions of the Stimulus will dramatically alter the application of HIPAA to covered entities, business associates, and vendors of personal health records and electronic health records.

Table 1: Subtitle D, Part I - Improved Privacy Provisions and Security Provisions

Sec. 13400 – Definitions		**SUBTITLE D ~ PRIVACY**
Sec. 13401 – Application of security provisions and penalties to business associates of covered entities; annual guidance on security provision	**Part I – Improved Privacy Provisions and Security Provision**	
Sec. 13402 –Notification in the case of breach		
Sec. 13403 - Education on health information technology privacy		
Sec. 13404 – Application of privacy provisions and penalties to business associates of covered entities		
Sec. 13405 – Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format		
Sec. 13406 – Conditions on certain contracts as part of health care operations		
Sec. 13407 – Temporary breach notification requirement for vendors of personal health records and other non-HIPPA covered entities		
Sec. 13408 – Business associate contracts required for certain entities		
Sec. 13409 – Clarification of application of wrongful disclosures criminal penalties		
Sec. 13410 – Improved enforcement		
Sec. 13411 – Audit		

Expanded Definition of Business Associate

The Stimulus extends the application of the main provisions of the HIPAA Security and Privacy regulations to business associates (Section 13401(a)), and contains expanded civil and criminal penalties for violation of the HIPAA Privacy and Security Regulations (Section 13401(b)). The Stimulus also requires the Secretary of the Department of Health and Human Services (HHS) to conduct periodic compliance audits of business associates as well as covered entities (Section 13401(c)).

The legislation also expands the definition of business associates to include organizations that provide protected health information as a data transmission service and those that require access to protected health information on a routine basis, as well as vendors who contract with covered entities to offer personal health records (PHR) to patients (Section 13408). The provisions of Section 13408 became effective on enactment of the Stimulus on February 17, 2009. Vendors of personal health records (*see e.g.* http://www.google.com/intl/en-US/health/about/), entities that offer products or services through the Web site of a vendor of personal health records, entities that access or send information in a personal health record, and third-party vendors of these entities also must comply with the HIPAA Privacy and Security Regulations (Section 13424(b)(1)(A)).

Security Breach Notification Requirement

The Stimulus includes a requirement for security breach notifications similar in form to laws passed by states with respect to information associated with identity theft. Section 13400 defines breach as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information." The definition of breach excludes situations where:

- The unauthorized person to whom such information was disclosed would not reasonably have been able to retain such information; and
- The information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without proper authorization.

Generally, prior to the Stimulus, a "covered entity" was not required to notify individuals of privacy or security breaches affecting personal health information. However, the Stimulus will require covered entities and business associates to notify both individuals and the Secretary of HHS of "unsecured protected health information" breaches. In the event that the breach affects more than 500 individuals, notification also must be made to prominent media outlets serving the state or jurisdiction in which the individuals reside. The Secretary of HHS is also required to post the notification on the HHS Web site.

"Unsecured protected health information" is defined, within section 13402(h)(1)(A), as PHI not secured through the use of a technology or methodology specified by the Secretary of HHS. The Secretary of HHS is required to issue and annually update guidance specifying technologies and methodologies that render PHI "unusable, unreadable, or indecipherable to unauthorized individuals" (Section 13402(h)(2)). If

the Secretary of HHS fails to issue this guidance within 60 days of enactment, the technology standard applied will be developed or endorsed by a standards-developing organization accredited by the American National Standards Institute.

The Secretary of HHS is required to promulgate interim final regulations within 180 days of the enactment of the Stimulus (enacted February 17, 2009). The new security breach notification requirements, within Section 13402, apply to breaches that are discovered 30 days after the date of publication of the interim-final regulations by the Secretary (Section 13402(j)). Similar security breach notification requirements, within Section 13407, become effective to vendors of personal health records (PHRs) to breaches that are discovered 30 days after the date of publication of interim final regulations (Section 13407(g)(1).

Table 2 (below) summarizes other key changes applicable to covered entities and now business associates in complying with the revised HIPAA privacy regulations. The provisions of Subtitle D, Part I of the Stimulus, entitled "Improved Privacy Provisions and Security - Provisions", become effective 12 months after the enactment of the Stimulus (February 17, 2010) (Section 13423) unless otherwise specified.

Table 2: Modifications to the HIPAA Privacy Regulations

Requirement	Prior to Stimulus	After the Stimulus	Relevant Cite
Right of Individual to Limit Access to PHI	Prior to the Stimulus, an individual had the right to request that the covered entity restrict certain disclosures of PHI, but the covered entity was not required to agree to the restriction.	A covered entity must comply with the individual's request to limit access to his/her PHI. This provision does not apply to the disclosure of PHI to a health plan for payment or health care operations where the health care provider has not been paid out of pocket in full.	Section 13405(a)
Minimum Necessary Standard	HIPAA privacy rule required covered entities to apply a minimum necessary standard to uses and disclosures of and requests for PHI.	The Stimulus requires the Secretary of HHS to issue guidance on what constitutes "minimum necessary" within 18 months after enactment. Provisions of this section apply six months after the date of the promulgation of final regulations.	Section 13405(b)
Accounting Requirement	The HIPAA privacy rule's accounting requirement did not include PHI disclosures for treatment, payment and health care operations purposes.	If a covered entity uses or maintains an electronic health records (HER), an individual will have the right to receive an accounting of disclosures made during the three years prior to the date of the request. A "reasonable fee" not greater than the entity's labor costs in responding to the request may be collected from the requesting party. This requirement would be effective as of January 1, 2014, for covered entities that have acquired an EHR prior to a certain date. For covered entities acquiring an EHR after that date, the requirement will be effective on the later of January 1, 2011 or the date the EHR is acquired.	Section 13405(c)
Individual Access to PHI in Electronic Form	Not Applicable	Requires covered entities that use or maintain EHRs to provide access of PHI to individuals in electronic format if requested.	Section 13405(e)(1)

Clarification of Penalties under the HIPAA Privacy and Security Regulations

Section 13410 of the Stimulus provides for a tiered increase of Civil Monetary Penalties (CMP) up to a maximum of $1.5 million depending on aggravating factors. The Stimulus also provides for the enforcement of HIPAA by State Attorney Generals. Many of these key provisions take effect after the enactment of the Stimulus including tiered monetary penalties and expanded enforcement provisions.

A wrongful disclosure under HIPAA (as modified by the Stimulus) occurs when a person obtains or discloses PHI maintained by a covered entity and the disclosing party has not obtained an authorization for the disclosure (Section 13409). The Stimulus requires that any CMP or settlement amount collected as a result of a privacy or security rule violation be transferred to the Office for Civil Rights to be used for enforcement of the HIPAA privacy and security rules and also in part to be distributed to those affected by the infraction (Section 13410(e)(1)).

Table 3: Tiered Civil Monetary Penalties

Standard of Culpability	Penalty	Maximum Penalty
Did not know of the violation and by exercising reasonable diligence would not have known of violation	Corrective action without penalty	No penalty--however, subject to discretion of Secretary.
Unknowing Violations	At least $100 per violation	Not to exceed $25,000 in a calendar year
Violation due to reasonable cause, not willful neglect	At least $1000 per violation	Not to exceed $100,000 in a calendar year
Violation due to willful neglect	At least $10,000 per violation	Not to exceed $250,000 in a calendar year
Violation is due to willful neglect and the violation is not corrected within 30 days of the first date the person liable for the penalty knew or should have known that the violation occurred.	At least $50,000 per violation	Not to exceed $1,500,000

Damages are calculated by multiplying the penalty by the number of violations in a calendar year for identical requirements or prohibitions. However, the total amount of damages shall not exceed the amount of the Maximum Penalty (Section 13410(d)(1)-(2)).

State Attorney Generals now have the authority to bring suit in federal district court against any person violating the rules on behalf of state residents to enjoin further violation or to obtain damages on behalf of such residents (Section 13410(e)). Statutory damages are limited to $100 per violation, not to exceed $25,000 in a calendar year for violations of identical requirements (Section 13410(e)(1)). The court may award attorneys fees to the state. The Secretary of HHS has the right to intervene in such actions.

* * *

For questions regarding this alert and topic, please contact:

Robert J. Hudock
Washington, DC
202/861-1893
rhudock@ebglaw.com

Mark E. Lutes
Washington, DC
202/861-1824
mlutes@ebglaw.com

The EpsteinBeckerGreen Client Alert is published by EBG's Health Care and Life Sciences practice to inform health care organizations of all types about significant new legal developments.

Lynn Shapiro Snyder, Esq.
EDITOR

If you would like to be added to our mailing list or need to update your contact information, please contact, Jennifer Sunshine, jsunshine@ebglaw.com or 202/861-1872.