BRADLEY ARANT BOULT CUMMINGS LLP

HEALTH CARE ALERT

Stimulus Bill Alters HIPAA Privacy and Security Rules; Federal Government Signals Renewed Interest in Enforcement of Rules

The American Recovery and Reinvestment Act of 2009 (commonly known as the Stimulus Bill), signed into law on February 17, makes several important changes with respect to the HIPAA privacy and security rules. These changes will require entities covered by the rules, their business associates and others to review and possibly revise their health information policies, procedures, practices and agreements. Further, through the Stimulus Bill and through the February 18 announcement of a settlement of a HIPAA privacy case against CVS, the nation's largest pharmacy chain, the federal government signals a renewed interest in the enforcement of the privacy and security rules.

Stimulus Bill

Here are just a few of the Stimulus Bill's key health information privacy and security provisions:

- *The Stimulus Bill significantly increases civil monetary penalties.*

Civil monetary penalties were limited under HIPAA to $100 for each violation of a provision up to a maximum of $25,000 per provision per year. Under the Stimulus Bill, civil monetary penalties are tiered based on the severity of the violation and the covered entity's response. The maximum penalty is now $50,000 per violation up to a maximum of $1,500,000 per provision per year.

- *The Stimulus Bill will dramatically alter the application of the HIPAA privacy and security rules to business associates.*

The privacy and security rules have not directly applied to the business associates of covered entities. Rather, the rules require covered entities to enter into agreements (commonly called "business associate contracts") with their business associates that impose on the business associates certain contractual obligations with respect to health information protected by the rules. The Stimulus Bill will directly subject business associates to the security rule's requirements. Those requirements are more detailed and probably more onerous than the contractual obligations found in the typical business associate contract. Business associates will need to review their administrative, physical and technical safeguards, their policies and procedures and their agreements with subcontractors to ensure compliance with the rule. Further, the Stimulus Bill provides that the same civil and criminal penalties that apply to covered entities apply to business associates that violate the security rule or a privacy or security provision of their business associate contracts.

- *The Stimulus Bill will impose new self-disclosure obligations on covered entities and*

business associates in the event of an information breach.

The Stimulus Bill imposes specific new self-disclosure obligations, which include notice both to the affected individual and to the Department of Health and Human Services ("HHS") and, depending on the number of individuals affected, also may require disclosure to prominent media outlets.

- *The Stimulus Bill will require the amendment of business associate contracts.*

The Stimulus Bill specifically provides that additional privacy and security requirements in the bill be incorporated into business associate contracts. Accordingly, covered entities may need to once again amend all of their business associate contracts.

- *The Stimulus Bill expands the information subject to a request for an accounting of disclosures.*

Under the HIPAA privacy rule, individuals are permitted to request from covered entities an accounting of the covered entities' disclosures of the individuals' health information. However, that accounting need not include disclosures for the purposes of treatment, payment or health care operations. The Stimulus Bill will require covered entities to account for disclosures for these purposes if the disclosures occurred in the 3-year period prior to the request and were made through an electronic health record. Covered entities will need to revise their policies and procedures to ensure compliance with this expanded accounting requirement.

- *The Stimulus Bill requires covered entities to agree to requests for restrictions on certain disclosures to health plans.*

Under the HIPAA privacy rule, covered entities are permitted to use and disclose protected health information without the individual's permission for treatment, payment or health care operations purposes. Covered entities are required to allow individuals to request restrictions on such uses and disclosures, but are not required to agree to those restrictions. The Stimulus Bill will require covered entities to comply with a request to restrict disclosures to a health plan for payment or health care operations if the information pertains solely to items or services for which the health care provider has been paid out of pocket in full.

- *The Stimulus Bill clarifies that individuals, and not just covered entities, are subject to HIPAA's criminal penalties.*

In 2005, the Department of Justice opined that only covered entities are subject to HIPAA's criminal penalties and that the penalties do not apply, for example, to the employee of a covered entity, even if the employee committed the act that violated HIPAA. The Stimulus Bill clarifies that an employee or other individual will be personally subject to HIPAA's criminal penalties if he or she obtains or discloses without authorization information maintained by a covered entity.

CVS Settlement

In addition to the changes in the Stimulus Bill, the Office of Civil Rights ("OCR") announced on February 18 that CVS has agreed to pay $2.25 million and to implement a robust corrective action plan. To settle claims that several CVS retail pharmacies inappropriately

disposed of protected health information in unsecured dumpsters. Prior to the CVS resolution agreement, OCR had entered into only one other health information privacy resolution agreement. In July 2008, Providence Health and Services agreed to pay $100,000 to settle claims arising out of Providence's loss of electronic backup media and laptop computers.

Bradley Arant Boult Cummings LLP Commentary

The Stimulus Bill and the CVS settlement may signal a resurgence in health information privacy and security compliance efforts. The Stimulus Bill's provisions will require HIPAA covered entities, their business associates and others to review, and most likely revise, their health information privacy and security policies, procedures, practices and contracts. Further, the bill and the CVS settlement suggest a renewed interest on the part of the federal government in the enforcement of the privacy and security rules. For example, in addition to the increased civil monetary penalties, the bill provides for periodic compliance auditing by HHS and enforcement of the rules by the State Attorneys General.

Most of the health information privacy and security provisions of the Stimulus Bill will not become effective for one year. However, because of the sweeping changes in the bill and because of the government's renewed interest in enforcement, affected organizations should begin analyzing their obligations now.

For more information on the Stimulus Bill's health information privacy and security provisions, please contact **Mark Lewis** or **Andrew Elbon**.

Bradley Arant eNews is published solely for the interest of clients and friends of Bradley Arant Boult Cummings LLP and should in no way be relied upon or construed as legal advice. The information contained herein is general in nature and based on authorities that are subject to change. If you need specific information on legal issues or want to address specific factual situations please seek the opinion of legal counsel.

No representation is made that the quality of the legal services to be performed is greater than the quality of legal services performed by other lawyers. Contact: John B. Grenier, Esq., 1819 Fifth Avenue North, Birmingham, Alabama 35203.

© 2009 Bradley Arant Boult Cummings LLP. All rights reserved.