O'Melveny

Alerts & Publications

The Stimulus Act Stimulates HIPAA Enforcement

January 1, 0001

The American Recovery and Reinvestment Act of 2009 (the "Stimulus Act"), signed into law by President Obama on February 17, 2009, implements a number of significant changes to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Stimulus Act affects the obligations and liabilities of business associates as well as covered entities and increases the penalties for HIPAA violations. This Client Alert highlights important HIPAA changes.

HIPAA Privacy and Security Provisions Apply to Business Associates

In a significant change from current law, the Stimulus Act explicitly applies HIPAA privacy and security provisions to business associates.
Currently, HIPAA regulations apply only to health plans, most health care providers, and clearinghouses (collectively defined as "covered entities") and govern the manner in which covered entities use, disclose and safeguard individuals' protected health information ("PHI"). While covered entities routinely contract with business associates to perform administrative services such as claims processing, practice management, and legal, actuarial, or accounting services, HIPAA regulations have not previously applied directly to business associates.

Rather, business associates simply entered into business associate agreements with covered entities under which business associates became contractually obligated to follow HIPAA privacy and security requirements. Consequently, business associates were not subject to the civil and criminal penalties under HIPAA, and their liability for violating HIPAA regulations was limited to contractual damages.

Under the Stimulus Act, business associates are now directly subject to both civil and criminal penalties for violations of certain HIPAA security and privacy requirements. As a result, business associates should carefully review their HIPAA practices and procedures for compliance.

State Actions Against HIPAA Violators are Authorized

Under current law, only the Department of Health and Human Services and the Department of Justice have the authority to pursue civil and criminal penalties for HIPAA violations. In a significant expansion of enforcement authority, the Stimulus Act permits state attorneys general to pursue civil actions against alleged HIPAA violators.
Specifically, state attorneys general may bring civil actions in federal court if there is reason to believe that the interests of one or more residents have been or are threatened or adversely affected by a HIPAA violation. States can seek both injunctive relief and monetary damages, and the court is authorized to award reasonable attorney fees to the state as well.

Additionally, the Secretary of Health and Human Services is directed to establish regulations within three years that allow individuals harmed by HIPAA violations to receive a percentage of any civil monetary penalties or settlements.

Increased Penalties for HIPAA Violations

The Stimulus Act creates four tiers of penalties for HIPAA violations tied to the culpability of the offender and generally increases the amount of monetary penalties offenders face. Under the new law, the Secretary may impose fines ranging from $100 up to $50,000 for each violation of HIPAA depending on whether a violation was inadvertent, reasonable, or due to willful neglect. The maximum penalty faced by an offender ranges from $25,000 to $1.5 million during a calendar year, again depending upon an offender's culpability.

Notification in the Case of Breach

The Stimulus Act imposes a new requirement on covered entities to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed as a result of a security breach. Notification must be made within 60 days of discovering the breach.
The Stimulus Act also requires covered entities to notify the Secretary of Health and Human Services regarding any unsecured protected health information that was acquired or disclosed in a breach. If a breach involves 500 or more individuals the covered entity must notify the Secretary immediately. If the breach affects fewer than 500 individuals, a covered entity may choose to notify the Secretary immediately or opt to create a log documenting such breaches to be submitted to the Secretary on an annual basis.

Business associates are also subject to notification requirements when they suffer a breach. Business associates are required to notify the corresponding covered entity and must provide the identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed as a result of a security breach. The covered entity is then responsible for notifying the affected individuals.

Effective Dates

The provisions extending security and privacy requirements to business associates are effective February 17, 2010.
In regard to the notification requirements, the Secretary must issue interim final regulations no later than 180 days after the effective date of the Stimulus Act. The notification provisions will apply to any breaches that are discovered 30 days after the interim regulations are published.

Finally, the provisions allowing for state actions against HIPAA violators and enhanced civil penalties are effective immediately.

Conclusion

In light of the increased penalties and enforcement for HIPAA violations, both covered entities and business associates should undertake a review of their HIPAA compliance measures, including business associate agreements and all policies, procedures, and practices related to the use, transmission, storage, and protection of PHI.