PUBLICATION

Stimulus Act Expands HIPAA Obligations and Enforcement Mechanisms

March 9, 2009

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (the Stimulus Act). Among the myriad topics contained in the Stimulus Act is the expansion of the obligations and enforcement mechanisms of the Health Insurance Portability and Accountability Act (HIPAA), and more specifically, HIPAA's Privacy and Security Rules. Below is a summary of the most significant changes to the HIPAA Privacy and Security Rules.

Business Associates Must Comply Directly with HIPAA's Privacy and Security Rules

Once only a requirement for "covered entities" (e.g., health plans, health care providers, and health care clearinghouses), HIPAA's Privacy and Security Rules will be directly applicable to "business associates" (any person or entity who, on behalf of a covered entity, performs or helps perform a function or activity involving the use or disclosure of protected health information (PHI)). Accordingly, on or before February 17, 2010, "business associates" must implement written security policies and procedures, physical security safeguards, and technical security safeguards for protected health information. Further, both "covered entities" and "business associates" should review relevant agreements to confirm that they comply with the Stimulus Act.

New Rules Regarding Security Breaches

With few exceptions, HIPAA's Privacy and Security Rules will be expanded to require covered entities and business associates to take affirmative steps in response to specified breaches of PHI. Specifically, both covered entities and business associates will be required to give written notification by mail or by e-mail (at the affected individual's prior election) "without unreasonable delay" and in no case later than 60 days after discovery of the breach. In the event current contact information is missing for the affected individual, notice of the breach will require posting on the company website and in other broadcast media.

For security breaches involving more than 500 individuals, a covered entity or business associate will be required to notify the U.S. Department of Health and Human Services (DHHS), and DHHS will post the name of the covered entity or business associate on its website. For security breaches involving more than 500 individuals in a particular area, a "prominent media outlet" must be notified.

Enhanced Civil Penalties and Enforcement, including DHHS Audits and State Attorneys General Enforcement Actions

The Stimulus Act significantly and immediately increases the amount of possible civil penalties. Penalties now range from $100 to $50,000 per violation based upon the nature of the violation, with caps for yearly maximum penalties now ranging from $1,000 to $1,500,000. Further, DHHS is required to conduct "periodic" audits of both covered entities and business associates. Since a portion of these increased penalties will go directly to fund the DHHS Office of Civil Rights, DHHS may indeed receive the requisite funding to increase the frequency of these audits. Moreover, the Stimulus Act provides state attorneys general with the authority to bring enforcement proceedings against any covered entity or business associate whose violations pose a threat to the citizens of their respective States and to recover attorneys' fees should the attorneys general

prevail on the merits. Accordingly, the number of audits and enforcement proceedings is likely to rise, and the penalties will be more severe.