BENESCH
Attorneys at Law

February 2009

STIMULUS BILL ALERT

Economic Growth and Development Team

HEALTH INFORMATION PRIVACY PROVISIONS IN THE STIMULUS BILL

Tucked into economic stimulation provisions of the Stimulus Bill is a set of changes to the health care information privacy rules created under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). (Stimulus Bill, Part A, Title XIII, Sections 13,400 *et seq.*) The HIPAA Privacy Rule set forth at 45 CFR Parts 160, 164 has long needed attention to various gaps that have been found in its treatment of protected health information ("PHI"), a concept referring to personally identifiable health information.

Generally speaking, the HIPAA Privacy Rule limits the use of a patients' PHI to uses connected with the patients' treatment, payment, public health matters, and other health care operations. Beyond these limited purposes, the patient has a general right to object to the disclosure of PHI.

The HIPAA Privacy Rule permits the disclosure of PHI to a limited category of "business associates" of health care providers and health plans, to enable these associates to fulfill support functions for the providers and health plans. However, the HIPAA Privacy Rule requires that each business associate execute a written contract ensuring that any PHI it receives will be appropriately safeguarded.

In addition to the privacy aspects of the HIPAA Privacy Rule, it also contains security standards designed to safeguard PHI in electronic form against unauthorized access, use, and disclosure. Those security standards have largely been codified in the Stimulus Bill.

The Stimulus Bill codifies the definitions of the following key privacy and security terms: breach; business associate; covered entity; disclosure; electronic health record; electronic medical record; health care operations; health care provider; health plan; National Coordinator; payment; personal health record; protected health information; secretary; security; state; treatment; use; and vendors of personal health records.

Certain of these terms have been modified from their original definitions in the HIPAA Privacy Rule. For example, "breach" has been redefined to make it clear that some inadvertent disclosures of PHI can be a breach.

A second modification is to the definition of "Personal Health Records" to clarify that PHR are "managed, shared and controlled by or primarily for the individual." This change excludes health related information maintained for commercial purposes, such as information maintained by life insurance companies.

The Stimulus Bill also addresses the administrative, physical and technical safeguard provisions of the HIPAA Privacy Rule, largely codifying these provisions with some important exceptions.

One of the most significant changes in the Stimulus Bill is that the HIPAA security standards, and the civil and criminal penalties for violating those standards, will now apply to "business associates" in the same manner they apply to the providers and health plans for which they are working.

An additional significant change is the imposition of a requirement that a breach of PHI security must be reported to each individual whose PHI was released in the breach. Moreover, if 500 or more individuals are impacted by a breach, a covered entity must report the breach to the Secretary of HHS and to major media outlets in the area that was impacted.

The Stimulus Bill also tightens other redisclosure aspects of the HIPAA Privacy Rule. In part, the Stimulus Bill addresses this issue by imposing stricter limitations on personal health information that is redisclosed in the form of limited data sets to third parties. The goals of these provisions is to generally avoid redisclosure of PHI unless the disclosure is specifically authorized by the individual and/or has been "deidentified" to protect the individual's identity.

The Stimulus Bill also addressed the continuing controversy over the use of PHI to market health care products and services. The existing HIPAA Privacy Rule generally bars the redisclosure of PHI to third parties for the purpose of

marketing health care products and services.

In the Stimulus Bill, covered entities will now be barred from using PHI in their possession for the purpose of marketing any health care products or services without the individuals consent, under most circumstances in which they receive payment from third parties for those marketing efforts. Similarly, covered entities will now be extremely limited in their use of PHI for fundraising purposes.

Finally, the Stimulus Bill dramatically strengthens the enforcement provisions of HIPAA, and enhances the penalties available. In the future, Justice Department enforcement will be backstopped by the OCR and potential actions by State Attorneys General.

Both OCR and the State Attorneys General will be permitted to seek civil monetary penalties, and the Attorneys General will also be permitted to seek injunctive relief for violations of the security and privacy standards of HIPAA, as modified in the Stimulus Bill.

For additional information, contact:

C. David Paragas
dparagas@beneschlaw.com
614.223.9307

William Todd
wtodd@beneschlaw.com
614.223.9348

Frank Carsonie
fcarsonie@beneschlaw.com
614.223.9361

www.beneschlaw.com