OBER | KALER
Attorneys at Law

Healthcare Privacy & Security Bulletin

February 10, 2009

Congress Includes Sweeping Expansion of HIPAA and Data Breach Notification Requirements In The Stimulus Bill

- Business Associates Would Become Subject To Important HIPAA Provisions and Penalties.

- Significant Provisions Affect Electronic Health Records, Health Information Exchanges and Personal Health Records

> ***"No man may rest secure in property or livelihood while Congress sits in session assembled"*** **- Mark Twain (attrib)**

Both the House and the Senate Versions of the America Recovery and Reinvestment Act of 2009 (the "Stimulus Bill") contain, as of February 7th, 2009, significant expansions of the HIPAA Privacy and Security Rules and other changes that, if enacted, will have a massive impact on the health care information and technology sector. While predicting the course of this legislation is risky given the larger issues it addresses, the broad similarities between the House and Senate provisions, coupled the Obama administration's emphasis on electronic health records bodes the inclusion of these provisions in any final legislation is likely, absent strong advocacy to the contrary by either consumer advocates or business advocates.

The principal provisions common to both the House and the Senate versions of the Stimulus Bill, subject to some minor differences, are as follows:

Business Associates Become Directly Regulated By HIPAA. Business Associates would become subject to the same requirements as Covered Entities for implementing administrative, physical and technical safeguards on Protected Health Information. In addition, Business Associates would be required to have written policies and procedures covering these requirements. Business Associates would become subject to the same civil and criminal penalties as Covered Entities.

This provision seems a logical step to close what the regulators viewed as a significant perceived "loop-hole" in the original HIPAA legislation passed in 1996: The law was limited to health plans, health care clearinghouses and health care providers who conducted core "back office" transactions in electronic form. HHS was limited to regulating the vast array of services providers who access or create Protected Health Information indirectly, through imposing the requirement that Covered Entities obtain "satisfactory assurances," in the form of a Business Associate Agreement" from such entities.

Notification of Data Breaches Involving PHI Becomes A Federal Law. Vendors Of Personal Health Records And Their Service Providers Made Subject To A Parallel NotificationRequirement. Through provisions that fundamentally replicate the "California" model for required notification of individuals about data breaches involving "personal information", the Stimulus Bill requires such notification by Business Associates to Covered Entities and by Covered Entities to Individuals in the event of such a breach involving Protected Health Information.

In many respects, these proposed Federal requirements are more rigorous than typical state laws. Notification must be given not later than sixty (60) days of when the breach is "discovered" and a breach is deemed discovered on the first day upon which the breach is known to the entity (including any employee, officer or other agent, other than the person that committed the breach). The burden of proof of compliance, including compliance with the timeliness of notice, is on the Covered Entity or Business Associate. In addition, notice to the Secretary of HHS is mandatory, and if the breach involves 500 or more individuals, must be given immediately.

The notification requirements only apply to information that is "unsecured", i.e. that is not secured through the use of a technology or methodology to be specified by the Secretary of HHS within sixty (60) days of the effective date of the law. Pending that, the standard for "secured" information requires compliance with an encryption methodology developed or endorsed by an ANSI accredited standards developing organization.

A separate provision of the Stimulus Bill imposes parallel requirements on entities that provide Personal Health Records and third party providers of services to those entities. Such vendors have successfully maintained that, since their information comes directly from the individual, they are not covered under HIPAA either as a Covered Entity or as a Business Associate, hence the separate provisions. Other differences are that the information which is covered is "PHR identifiable health information", that agency identification of breaches goes to the Federal Trade Commission, and that failure to comply is an "unfair and deceptive trade practice" enforceable within Federal Trade Commission jurisdiction.

Individuals May Require Covered Entities Not To Disclose Self Pay Services To Health Plans. Under the Privacy Rule as it presently exists, an individual has a right to request special privacy protections for Protected Health Information, but a Covered Entity is not required to grant that request, although the individual's request is retained in the record. Under the Stimulus Bill, a Covered Entity would be required to agree to an individual's request for privacy protections as to the disclosure of Protected Health Information for payment or health care operations if the information pertains only to a health care item or service that the individual has paid for out of pocket, unless otherwise required by law.

This provision answers one of the pervasive consumer concerns voices about Health Care Information Exchanges – that individuals may not want their insurance companies to know about some health care treatments for which the individuals are willing to pay out-of-pocket, so that the treatment will not affect the individual's insurance rates or insurability.

Pending Regulatory Guidance From HHS, the Limited Data Set Becomes The Default Minimum Necessary Standard "To The Extent Practicable." HIPAA regulates a Covered Entity's uses and a Covered Entity's disclosures of Protected Health Information. For non-treatment and most other disclosures, Covered Entities are required to use, disclose and request only the "minimum necessary" amount of Protected Health Information. The Stimulus Bill would give the Secretary of HHS an eighteen (18) month period to develop "guidance" on what constitutes the minimum necessary amount Protected Health Information. During that period, a HIPAA Limited Data Set would, to "the extent practicable" be the default standard for what complies with the minimum necessary requirement. A Limited Data Set is Protected Health Information from which all direct patient identifiers have been removed.

This provision will sunset when the Secretary issues guidance on the minimum necessary standard, but in the interim, considering the significant retooling of health care information policies and software systems within Covered Entities that elimination of direct patient identifiers would required, that emphasis in the health care industry is likely be on what is "practicable" and when is another "minimum necessary" data set appropriate for a given purpose.

Covered Entities Using Electronic Health Records Are Required To Provide Accounting Of Disclosures Of Protected Health Information For Treatment, Payment and Health Care Operations. Effective Date Is Delayed. At present, HIPAA exempts a Covered Entity's obligation to provide individuals with an accounting of disclosures of their Protected Health Information if the disclosure was for treatment, payment or health care operations. The Stimulus Bill provides that this exception would no longer be available to Covered Entities that use electronic health records. In recognition of the

burden that this is likely to impose, the period for which an accounting is required is limited to three (3) years, not the six (6) year period otherwise required. Still, this is a major change for all manner of Covered Entities.

In apparent recognition of the operational impact that this provision would have on the systems, including the software systems, that Covered Entities and their technology vendors have in place to capture data required for HIPAA accountings, the effective date of this provision is delayed until after January 14, 2014 (the expiration date of the Stark EHR donation exception and the parallel antikickback Safe Harbor) for Covered Entities that acquired electronic health records as of January 1, 2009. For entities that acquire electronic health records after January 1, 2009, the provision will be effective on the later of January 1, 2011 or the date upon which the entity acquires the electronic health record.

Health Information Exchanges Are Brought Specifically Within Business Associate Requirements. While arguably more a clarification than a change, an organization that provides data transmission of Protected Health Information to a Covered Entity (or its Business Associate) and that requires access to Protected Health Information in order to do so, such as a Health Information Exchange or a Regional Health Information Organization, is a Business Associate of participating Covered Entities. This provision also applies to vendors who provide Personal Health Records functionality to Covered Entities as a part of an electronic health records system.

Other Significant Provisions. The Stimulus Bill contains a number of other significant provisions:

In a clear push to broaden the use of de-identified information, the Secretary of HHS is directed to promulgate regulations within eighteen (18) months after enactment of the law that eliminates from the definition of Health Care Operations, activities that the Secretary determines could "reasonably and efficiently" be conducted using deidentified information.

The Stimulus Bill contains several provisions that directly affect marketing or similar communications.

- The Bill affirms that use of Protected Health Information for marketing communications are not within the scope of Health Care Operations, i.e. are not permitted without a HIPAA compliant authorization from each individual, unless it is within one of the three existing exceptions (health related products or services, treatment, or case management or care coordination). However, this is specifically narrowed by a provision that a Covered Entity or a Business Associate is prohibited from receiving direct or indirect payment in exchange for making any of those Health Care Operations marketing communications, except

payment to a Business Associate pursuant to a written contract with the Covered Entity or payment disclosed in a HIPAA compliant Authorization from the subject individuals. This is one area in which there are some significant differences between the House and the Senate versions.

- Fundraising for the benefit of a Covered Entity is no longer permitted under Health Care Operations.

- Covered Entities are prohibited from receiving direct or indirect remuneration for the sale of protected health information, without each individual's HIPAA compliant authorization. The provision is subject to a number of exceptions. The addition of indirect remuneration seems a departure from, or at least a significant clarification of, existing HIPAA Privacy Rule requirements, particularly in view of the exceptions. For example, consideration for the transfer of Protected Health Information for treatment of the subject individual or in connection with research or public health activities is exempt, so long as the remuneration reflects "not more than the costs of preparation and transmittal of the data." The fact that these exceptions needed to be specifically stated seems to indicate a specific and significant scrutiny of transfers of Protected Health Information for consideration, particularly if those transfers are cloaked as a transaction permitted under HIPAA.

- The Stimulus Bill clarifies that wrongful disclosures of individually identifiable protected health information are criminal, under the relevant provisions of the Social Security Act.

- The House version of the Stimulus Bill contains a provision that specifically provides that nothing in the Bill prevents a pharmacist from communicating with individuals in order to reduce medication errors and improve patient safety, provided that there is not remuneration other than for the treatment of the individual.

- Finally, the Secretary of Health and Human Services is directed to establish Privacy Advisors in its regional offices.

For more information about health care privacy and security issues, contact James B. Wieland, a principal in the Health Law Group at Ober|Kaler, at jbwieland@ober.com.