Healthcare Information Privacy, Security and Technology Bulletin

February 19, 2009

The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"): Congress Includes Sweeping Expansion of HIPAA and Data Breach Notification Requirements in the Stimulus Bill

HIPAA Covered Entities and Business Associates affected. Personal Health Records (PHR), Electronic Health Records (EHR) and Health Information Exchanges (HIE) subject to new federal requirements.

The American Recovery and Reinvestment Act of 2009, the "Stimulus Bill," includes Title XIII – "Health Information Technology," also known as the "Health Information Technology for Economic and Clinical Health Act" or "HITECH Act." The HITECH Act contains significant expansions of the HIPAA Privacy and Security Rules and numerous other changes that will have a major impact on the health care information and technology sector. Virtually every health care provider and third party service provider that stores or accesses individuals' medical information will be affected by this new federal law.

This Ober|Kaler Health Information Privacy, Security and Technology Bulletin provides an overview of Subtitle D of the HITECH ACT: "Privacy," particularly Part 1 "Improved Privacy Provisions and Security Provisions."

Effective Date

Except where otherwise specifically provided, the effective date of the Improved Privacy Provisions and Security Provisions discussed in this bulletin appears to be twelve (12)

months after enactment[1]. However, as noted below, there are a number of provisions with different effective dates.

Business associates will be subject to HIPAA security provisions and to sanctions for violation of business associate requirements.

- The HIPAA requirements for administrative, physical and technical information safeguards and written policies and procedures will apply directly to Business Associates as well as civil and criminal penalties for violations. The Secretary of HHS will publish annual guidance on "the most effective and appropriate technical safeguards" for this purpose.

- Other HITECH Act security provisions also apply. As discussed below, Business Associates must detect and report "security breaches" to covered entities.

- The HIGHTECH Act also provides that a Business Associate that obtains or creates Protected Health Information pursuant to a written contract or arrangement may use or disclose Protected Health Information *only* "in compliance with each applicable requirement of [45 CFR] 164.504 (e)." The cited section contains the detailed implementation requirements for a Business Associate Agreement as well as the requirement for action in the event of knowledge of a "pattern of activity or practice" that is a material breach of the Business Associate agreement. In other words, whatever the Business Associate Agreement provides or does not provide, Business Associates will directly responsible for full compliance with the relevant requirements of the Privacy Rule itself, and subject to civil and criminal penalties if they fail to do so.

- This provision, in conjunction with the provisions regarding notification of security breaches discussed in the next section will have a major, long them impact on service providers who work with Protected Health Information, the "non-covered entity" sector of the health information system. This provision closes what was perceived by regulatory authorities as a significant gap in the jurisdictional ambit of HIPAA. As originally written, HIPAA was limited to health plans, health care clearinghouses and health care providers who conducted core "back office" transactions in electronic form. Third party service providers were not initially subject to direct regulation.

---

[1]Subtitle D is divided into Part 1 'Improved Privacy Provisions and Security Provisions" and Part 2 "Relationship to Other Laws; Regulatory References; Effective Date; Reports." Section 13423, in Part 2 in the Conference Committee draft and in the final version states, in relevant part, "Except as otherwise provided, the provisions of part I shall take effect on the date that is 12 months after the date of the enactment of this title" (emphasis added). Given the structure, Congressional intent seems clear, although there is no part [Roman Numeral] I.

Federal law now requires consumer notification of data breaches involving "*unsecured*" PHI. Both covered entities and business associates must comply.

- The breach notification provisions are effective for breaches that occur 30 days after the Secretary of HHS publishes implementing interim final regulations. These regulations are due within 180 days after enactment.

- The notification protocol generally follows the "California model" of notification already adopted by the majority of states. However, the new federal notification requirements are more stringent than the notification laws of many states in several respects:

    - The breach is deemed discovered on the *first day* that the breach is known or should reasonably have been known to the entity, including to any employee, officer or "other agent" (other that the individual committing the breach).

    - Individual notification must be provided within *sixty days* of discovery, absent a law enforcement official's instructions to the contrary.

- In addition to notice to affected individuals, Covered Entities must also notify the Secretary of HHS of a breach of security. This notice must be provided *immediately* if the breach involves 500 or more individuals. Covered Entities may maintain a log of breaches involving less than 500 individuals, and provide the log to the Secretary of HHS annually. The Secretary will post a list of Covered Entities providing a notice of breaches involving 500 individuals or more on its website.

- Business Associates must report a security breach to the Covered Entity under the within the same time frame. A Business Associate who fails to do so will be subject to direct enforcement and penalties.

- "Unsecured" PHI is PHI which is not protected by "technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals," i.e., in lay terms, PHI that is not encrypted. The Secretary of HHS is directed to develop standards for securing PHI within 60 days of enactment. A default definition is provided, in the event that the Secretary does develop the standards in a timely manner. The default standard is the same as the above quoted language, with the additional requirement that the technology or methodology be developed or endorsed by an American National Standards Organization approved organization.

- The burden of proof of compliance, including compliance with the timeliness of notice, is explicitly on the Covered Entity or Business Associate.

Vendors of personal health records and their service providers made subject to the same security breach notification requirement

- These provisions are captioned in the HIGHTECH Act as "Temporary." They have the same Effective Date as the parallel provision for Covered Entities and Business Associates. However, the PHR Vendor provisions sunset if Congress enacts new legislation establishing requirements for security breach notification for entities that are not Covered Entities or Business Associates.

- A PHR vendor has the same obligations as to security breaches as a Covered Entity and a third party service provider has the same obligations as a Business Associate.

- A "Personal Health Record" is "an electronic record of PHR identifiable health information . . . on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual." "PHR identifiable health information," is Protected Health Information held by a PHR vendor or service provider. A third party service provider is an entity that provides services to the vendor in connection with the offering or maintenance of a PHR *or* a related product or service *and* that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHR identifiable health information in such a record as a result of such services."

- This notification requirement applies to the PHR identifiable information of a "citizen or resident of the United States."

- Breaches related to a Personal Health Record are initially reported to the Federal Trade Commission; the FTC will notify the Secretary of HHS. Failure of a PHR vendor or a service provider to comply with the requirements of this section is an "unfair and deceptive trade practice" enforceable within Federal Trade Commission jurisdiction.

Individuals may require Covered Entities not to disclose certain self pay services to health plans.

- Under the Privacy Rule pre-HITECH Act, an individual has a right to request restrictions on disclosure of the individual's 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 HIGHTECH Act, a Covered Entity is *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 in full, *unless* disclosure is otherwise required by law or is for treatment purposes.

- This provision answers one of the consumer privacy concerns about Health Care Information Exchanges (HIEs) (f/k/a Regional Health Information Networks – RHIOs) – that individuals might not want their insurance companies to know about certain health care services out of concern that the treatment would affect the individual's insurance rates or insurability.

The limited data set becomes a default minimum necessary standard.

- 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 HITECH Act provides that, in order to be treated as in compliance with the HIPAA minimum necessary requirements, a Covered Entity must limit its requests for and use or disclosures of Protected Health Information to (i) a "Limited Data Set" *"to the extent practicable,"* or (ii)*"if needed by such entity"*, (i.e. apparently, the Limited Data Set is not "practicable") to the minimum necessary to accomplish the intended purpose of such use, disclosure or request.

- The current exceptions to the minimum necessary requirement continue to apply, including disclosures for treatment purposes, continue to apply.

- The Limited Data Set has, to date, mainly been the concern of entities engaged in research. A Limited Data Set is still Protected Health Information under HIPAA, but all "direct identifiers" have been removed.

- The Secretary of HHS is directed to issue guidance on what constitutes the minimum necessary within eighteen (18) months of enactment. This provision sunsets after those regulations are issued.

Covered Entities using electronic health records ("EHR") are required to provide accounting of disclosures of protected health information for treatment, payment and health care operations.

- HIPAA, pre HIGHTECH Act, exempted a Covered Entity from an obligation to provide individuals with an accounting of disclosures of their Protected Health

Information if, among other things, the disclosure was for treatment, payment or health care operations.

- Under the HIGHTECH Act, this exception is eliminated as to Covered Entities that use EHR.

- For disclosures by a Business Associate, the Covered Entity may provide the accounting or may direct the individual to its Business Associates, who must comply with the accounting requirements.

- 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.

- The effective date of this provision is delayed, as follows:

    - For Covered Entities, insofar at they acquired an EHR as of January 1, 2009, the accounting requirement applies to disclosures made on or after January 14, 2014.

    - For Covered Entities insofar as they acquired EHR after January 1, 2009, the provision will be effective for disclosures on the later of January 1, 2011 or the date upon which the entity acquires the electronic health record.

    - The Secretary of HHS can impose a later effective date but it can be no later than 2016 for the Covered Entities with EHR as of January 1, 2009 and 2013 for all other Covered Entities with EHR.

Health Information Exchanges are brought specifically within Business Associate requirements.

- While arguably not a change in the law, the HIGHTECH Act specifically provides that 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 ("HIE") or a Regional Health Information Organization ("RHIO"), is a Business Associate of participating Covered Entities. This is consistent with Guidance recently provided by the Office of Civil Rights.

- This provision also applies to vendors who provide Personal Health Records functionality to Covered Entities as a part of an electronic health records system,

Restrictions on the remuneration for "sale" of Electronic Health Records or Personal Health Information

- A Covered Entity or a Business Associate cannot "directly or indirectly" receive remuneration in exchange for *any* Protected Health Information of an individual *except* pursuant to a valid HIPAA authorization that include specifics on any further exchanges of the Protected Health Information by its recipient.

- Presumably, consistent with earlier, unrelated comments of the Secretary of HHS, the federal fraud and abuse test for what constitutes direct or indirect remuneration will apply.

- The HIGTTECH Act provides a number of exceptions to this prohibition:

    - Transfers for public health activities, as defined by HIPAA

    - Transfers for research purposes, subject to limitations on the remuneration

    - Transfers for treatment, unless the Secretary of HHS determines otherwise

    - Transfers in connection with the sale or merger of a Covered Entity

    - Remuneration that is paid by the Covered Entity to a Business Associate related to the Business Associate's services as to the exchange of PHI

    - Providing an individual with a copy of the individual's PHI

    - Other situations, as determined by the Secretary.

- This provision of the HIGHTECH Act is effective only for exchanges that occur six months after the Secretary of HHS promulgates implementing regulations. The Secretary is directed to promulgate those regulations within 18 months of enactment.

Covered Entities with Electronic Health Records must provide an individual's information in electronic form and transmit it to third parties, on the individual's request.

- If an individual requests a Covered Entity that has an EHR, that Covered Entity must:

  - Provide the individual with a copy of the individuals information in electronic format
  - If the individual directs, the Covered Entity must also transmit the copy directly to a recipient designated by the individual

  - The fee that a Covered Entity can charge is limited to its "labor costs."

- This provision will clearly simplify the ability of an individual to transport information form the individual's treatment providers to the individual's Personal Health Record.

The HIPAA Health Care Operations exception for "marketing" communications is narrowed significantly, if direct or indirect remuneration is received.

- Pre-HITECH Act, an individual could provide communications that might otherwise be considered marketing without individual authorization *if* the communication was to describe a health care item or service or third party payment for the item or service, for treatment, or for case management or counseling about alternative treatments. These activities were considered Health Care Operations.

- Under the HITECH Act, such communications are not Health Care Operations, *if* the Covered Entity or Business Associate making the communication receives "direct or indirect remuneration" for making the communication. As discussed above, the relatively broad federal fraud and abuse definition of remuneration is likely to apply. Payment for treatment, however, is specifically not remuneration for this purpose.

- This change does not apply, if:

  - The communication is about a current drug or biological the recipient is taking, under certain circumstances, if the remuneration is "reasonable," a term to be defined by the Secretary of HHS

  - The communication is made by the Covered Entity based on a valid HIPAA authorization

  - The communication is made by a Business Associate of the Covered Entity in accordance with a written Business Associate Agreement

Individuals must be given a right to opt-out of receipt of Covered Entity's fund raising communications

- In a change from earlier versions, the HIGHTECH Act continues the right of Covered Entities to use and disclose Protected Health Information for fundraising purposes, as a permitted Health Care Operations activity.

- However, individuals must be provided, in a "clear and conspicuous manner," with a right to opt-out of receiving further fundraising communications.

- An individual who opts out will be treated as having revoked an authorization.

The Act provides for "Improved Enforcement"

- The Act amends the Social Security Act to add a provision requiring the Secretary to "formally investigate any compliant of a violation of this part if a preliminary investigation of the facts of the complaint indicate such a possible violation due to willful neglect" (sic).

- The Act clarifies that for purposes of the definition of wrongful disclosure "a person (including any employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization."

For more information about health care information privacy, security and technology issues, contact James B. Wieland, a principal in the Health Law Group at Ober|Kaler, at jbwieland@ober.com or at 410-347-7397. Jim heads Ober|Kaler's Health Care Information Privacy, Security and Technology Group.