By Bob Doe

HITECH Meets HIPAA

HITECH Act Changes to HIPAA Obligations for Covered Entities and Business Associates

In addition to providing economic stimulus incentives related to adoption of EHR systems, Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), otherwise known as the Health Information Technology for Economic and Clinical Health Act (HITECH), sets forth a number of new or modified HIPAA obligations. The purpose of this article is to summarize some of the more significant changes. This information should be used as a starting point to determine what changes may apply to you and/or your organization. Additional review and discussion with legal counsel will be necessary.

Application to Business Associates (effective Feb. 17, 2010). The administrative safeguards, physical safeguards, technical safeguards, and policies and procedures documentation requirements of HIPAA that previously applied only to covered entities now apply directly to business associates (both covered entities and business associate are defined terms within HIPAA). The additional security requirements added by HITECH are also applicable to business associates and should be incorporated into the business associate agreement between the covered entity and the business associate. The Secretary of Health and Human Services is to provide annual guidance on the most effective and appropriate way to achieve these standards.

Breach Notification (approximate effective date: September 2009). HITECH requires a covered entity to make specific notification to each individual in the event the individual's "unsecured protected health information," as defined by HITECH, has been, or is reasonably believed to have been, disclosed as a result of a breach. "Unsecured protected health information" is defined as information that is not secured through the use of technology or methodology specified by the Secretary of Health and Human Services (the "Secretary") that renders the information unusable, unreadable or indecipherable to unauthorized individuals. Business associates must notify the covered entity in the event the business associate discovers such a breach. Breach occurs on the first day it is known, or should reasonably have been known, by any person other than the person committing the breach, including any employee, officer or agent of the covered entity or business associate. All notifications must occur without unreasonable delay but in no event more than 60 days after discovery of the breach. If contact information for 10 or more such individuals is out of date, the notice must be made on the covered entity's Web site or major print or broadcast media. If the breach involves more than 500 people, the notice must be published in prominent media outlets and the information will also be posted on the Secretary of Health and Human Services Web site. As a result of these changes, covered entities should consider providing training for employees and agents regarding the reporting of breaches. In addition, covered entities should endeavor to keep all contact information up to date to avoid unnecessary public exposure.

Direct Application of HIPAA Requirements to Business Associates (effective 12 months after ARRA enactment). Prior to HITECH, a business associate's use of protected health information was governed by the business associate agreement with the covered entity. HITECH

requires that any protected health information (PHI) obtained by way of a business associate agreement, can be used and disclosed only if such use and disclosure complies with the provisions listed in HIPAA that must be included in each business associate agreement. Business associates may also be found in violation of HIPAA in the event they fail to take action upon becoming aware that the covered entity is not in compliance with HIPAA. In effect, this provision subjects business associates directly to the business associate provisions of HIPAA, in addition to the contractual obligations it has with the covered entity. Business associates also can be subject to civil and criminal penalties under HIPAA. In addition, the additional privacy requirements created by HITECH also will be applicable to such business associates and should be incorporated into the business associate agreement. Covered entities and business associates should review their business associate agreements with legal counsel in order to make the appropriate modifications.

Restrictions on Disclosures of Protected Health Information (effective 12 months after ARRA enactment). Prior to HITECH, individuals could request restrictions on the use of their PHI for treatment, payment, or healthcare operations, but covered entities were not required to comply with the request. HITECH now requires covered entities to comply with such a request if it is a disclosure to a health plan that is not treatment-related and the health care provider has been paid out of pocket in full for the item or services provided related to the PHI.

Minimum Use Restrictions (effective 12 months from ARRA enactment). HITECH provides additional definition as to the term "minimum necessary" as it relates to the HIPAA requirement that, in certain, limited, scenarios, a covered entity use, disclosure or request only the minimum necessary PHI to accomplish the intended purpose. HITECH provides that the covered entity limit the PHI, to the extent practicable, to the limited data set (as defined in HIPAA; basically de-identified data), or to the minimum necessary to accomplish the intended purpose. However, the Secretary will issue guidance as to what constitutes "minimum necessary" and this will override the definition stated above.

Sale of PHI (effective six months from ARRA enactment). HITECH prohibits the sale of PHI unless such sale is described in one of the listed exceptions.

New Accounting Requirements (effective for current EHR users Dec. 1, 2014; for those acquiring an EHR after Jan. 1, 2009—the later of Jan. 1, 2011, or the date the EHR is acquired). With regard to covered entities that use or maintain an electronic health record for PHI, HITECH removes the exception for providing an accounting for disclosures based on treatment, payment and healthcare operations. Such an accounting only applies to a period of three years prior to the date the accounting is requested.

Request for PHI (effective 12 months after ARRA enactment). HITECH now allows individuals to obtain a copy of their PHI in electronic format from a covered entity that uses or maintains an EHR with respect to PHI. The covered entity cannot charge a fee for these services in excess of the labor costs required to respond to the request.

Marketing Communications Rules (effective 12 months after ARRA enactment). With regard to communications that market products or services. HITECH further limits the number of communications that will be considered healthcare operation disclosures.

Improved Enforcement (effective on ARRA enactment). With regard to HIPAA violations due to willful neglect, HITECH has added mandatory penalties and mandatory investigation by HHS.

Penalties (effective on ARRA enactment). HITECH also increases penalties for HIPAA violations by covered entities and business associates based on the knowledge of the violation. HITECH provides for different penalties based on the category of the violation (i.e., no knowledge of a violation, violations due to reasonable cause, and violations due to willful neglect). HITECH also extends criminal penalties to individuals that obtain or disclose PHI without authorization. HITECH also authorizes state attorneys general to bring suit on behalf of its residents, and allows courts to award damages, costs and attorneys' fees in relation to the violations.

Audits (effective on ARRA enactment). HITECH also requires the Secretary to provide for periodic audits to ensure that covered entities and business associates comply with the requirements applicable to such organizations.

The foregoing summary is intended to provide an overview of the changes HITECH makes to existing HIPAA obligations. Covered entities and business associates will need to create and/or revise existing privacy and security policies and procedures and review and revise existing business associate agreements to ensure compliance. **JHIM**

Bob Doe is a founding member of the law firm of Bonnabeau, Salyers, Stites & Doe (www.bssdlaw.com) located in Minneapolis. Mr. Doe has extensive experience preparing, reviewing, and negotiating information technology contracts and can be reached at rdoe@bssdlaw.com or 952-548-6064.