

- Demonstrate that the certified EHR technology is connected in a manner that provides for the electronic exchange of health information; and
- Submit information on clinical quality measures and other measures in a form and manner that will later be specified by the HHS Secretary

A physician or hospital can demonstrate that it is a “meaningful EHR user” in the following ways:

- An attestation;
- The submission of claims with appropriate coding (such as a code indicating that a patient encounter was documented using certified EHR technology);
- A survey response; and
- Other means specified by the Secretary

While the HITECH Act offers a tremendous financial benefit to physicians and hospitals if they choose to implement EHR technology, several questions remain, including:

- Will physicians and hospitals who already implemented EHR technology be eligible to receive the payment incentives?
- Will the payments be made on a “first-come, first-served” basis?
- Will Florida law allow physicians to share the expenses of implementing EHR technology?

These questions will be answered by regulations to be released in the Federal Register before December 31, 2009.

For a more detailed analysis of the HITECH Act and its benefit to your practice or hospital, please see our upcoming Stimulus Bill Legal Update. Trenam Kemker’s Health Law Group will continue to monitor the HITECH Act and will keep our clients apprised of additional changes. ■

Modifications to HIPAA Contained in the Stimulus Bill



By: Jackie Crain

The Stimulus Bill sets forth a number of changes to the privacy and

security regulations implemented under the Health Insurance Portability and Accountability Act (“HIPAA”). In short, the changes strengthen the enforcement of HIPAA, expand the penalties or consequences of violations, and, most notably, impose new requirements and penalties on “business associates.” Accordingly, most business associate agreements will need to be amended. HIPAA-regulated covered entities and business associates need to be aware of the new enforcement authority provided to state attorneys general and the changes to the HIPAA requirements related to accessing protected health information (“PHI”), accounting for disclosures of such information and notifying individuals in the case of a breach of unsecured PHI.

Enforcement and Penalties

The Stimulus Bill gives authority to state attorneys general to bring suit in federal

court on behalf of the state’s residents to enjoin any person violating the HIPAA rules from committing continuing violations. The attorneys general are also permitted to seek damages on behalf of residents, and to obtain attorney’s fees.

Moreover, the Stimulus Bill clarifies that, in addition to covered entities themselves, employees or other individuals involved in violations are subject to the criminal penalties associated with HIPAA, and that obtaining or disclosing PHI “without authorization” is an offense for which penalties may be imposed. The Stimulus Bill also contains a requirement that the U.S. Department of Health and Human Services (“HHS”) use civil monetary penalties and settlement amounts for enforcement purposes and that a methodology is established to distribute a percentage of the civil monetary penalties to the individuals harmed by a HIPAA violation. Similar to what already occurs in “quitam” cases.

HHS also is required to provide for periodic compliance audits of covered entities and business associates.

Application of Provisions and Penalties to Business Associates of Covered Entities

The Stimulus Bill also expands the reach of HIPAA’s security rules and penalties to cover business associates. Under HIPAA, a “business associate” is a person (or organization) to whom a covered entity discloses PHI so that the person can carry out, assist with the performance of, or perform a function or activity for or on

behalf of the covered entity (examples include consultants, attorneys, accountants, third party administrators, management/billing companies, software providers). Under the new law, business associates will need to comply with the standards and implementation specifications related to administrative, physical and technical safeguards for electronic PHI and prepare policies and procedures to prevent the improper disclosure of PHI.

Business associates also will have a legal obligation to comply with the privacy regulations at 45 C.F.R. 164.504(e). Thus if PHI is used or disclosed in a manner that is contrary to HIPAA, the business associate will be in violation of the law and subject to penalties, as opposed to simply being subject to a breach of contract claim by the covered entity.

The new language clearly establishes that business associates will be subject to the same HIPAA criminal and civil penalties that covered entities are subject to for a violation of any privacy or security provision (Originally HIPAA set these at \$100 per violation up to \$25,000 per year in civil penalties and fines of up to \$250,000 and/or imprisonment up to 10 years for knowing misuse of PHI.).

Breach Notifications

Like the many new state laws requiring notification to consumers of security breaches, the Stimulus Bill imposes a legal duty on covered entities and business associates to notify

certain parties of a breach of unsecured PHI, which is defined to mean the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security, privacy, or integrity of the PHI. This duty appears to apply to unencrypted PHI, but the term 'unsecured' has not yet been clearly defined (the term unsecured PHI is described as PHI that is not secured through the use of a technology or methodology specified by HHS).

The required notices can involve written notices to individuals sent via mail or email, a posting on the home page of the organization's website or an announcement in a major print or broadcast media. Business associates are required to notify covered entities following the discovery of a breach of unsecured PHI. Notices must be sent "without unreasonable delay" and in no case later than 60 calendar days after the discovery of a breach. Breaches are considered discovered as of the first day on which the breach is known or should reasonably have been known to the entity or any person that is an employee, officer, or other agent of the entity – other than the person committing the breach. If the breach involves more than 500 individuals, then notice must be provided to a prominent media outlet and HHS. HHS will immediately post the information to its website. The notice of a breach to individuals (whether sent or posted) must include, to the extent possible: (1) a brief description of the facts surrounding the breach, including the date of the breach and date of the discovery of the breach; (2) a description of the

types of unsecured PHI involved, such as full name, SSN and home address; (3) the steps individuals should take to protect themselves from potential harm associated with the breach; (4) a brief description of the measures taken to investigate the breach, mitigate losses, and prevent further breaches, and (5) contact information for questions, including a toll-free telephone number, an email address, website, or postal address.

These requirements may not be aligned with state security breach notification laws and they are significantly different from the current HIPAA regulations, which do not require any notice to individuals by the covered entity unless the covered entity determined that the notice was necessary to mitigate damages to the individual.

Access to Certain Information; Accounting of Certain PHI Disclosures

Individuals have a right to inspect or receive a copy of their PHI contained in a covered entity's designated record set. Furthermore, individuals have a right to receive an accounting or list of certain disclosures of their PHI (e.g. disclosures other than those for treatment, payment, or healthcare operations or those made to, or authorized by, the individual). The Stimulus Bill expands these rights and gives individuals the right to obtain information in electronic format if the covered entity uses or maintains electronic health records ("EHRs") and a right to obtain an accounting of any disclosure of PHI

related to the EHR during the three years prior to the date of the request.

New Definitions Coming

Under HIPAA, covered entities are required to limit the unauthorized use and disclosure of PHI to the minimum amount necessary for the intended purpose (unless the disclosure is for treatment). The Stimulus Bill requires HHS to develop new guidance on what constitutes the “minimum amount necessary.” HHS is also obligated to review the definition of healthcare operations and eliminate from the definition any “operations” activity that can be reasonably performed by using de-identified information.

Other Changes or Requirements

- HHS shall annually issue guidance on technical safeguards and the HIPAA security standards. This includes guidance specifying the technologies and methodologies that will render electronic PHI secure or unusable, unreadable or indecipherable to unauthorized individuals.
- A covered entity must comply with an individual’s requested restriction to his/her PHI if: (a) the disclosure is to a health plan for purposes of carrying out payment

or operations (and not for treatment), and (b) the PHI pertains to a health care item or service for which the provider was paid in full.

- The sale of electronic health records or PHI obtained from electronic health records is in most cases prohibited.
- The HIPAA regulations related to marketing are more stringent; an individual’s authorization is generally required if a covered entity or business associate directly or indirectly receives remuneration in exchange for PHI.
- The new law applies HIPAA beyond covered entities and business associates to personal health record vendors. These personal health record vendors must notify individuals and the Federal Trade Commission following the discovery of a security breach of unsecured personal health records and the failure to do so may be treated as an unfair and deceptive act or practice.
- The new law sets forth a tiered increase in the amount of civil monetary penalties for HIPAA violations. The increases are dramatic compared to the current amounts and these new amounts are effective immediately (e.g. the \$100 per violation noted above will be

increased to \$1,000 per violation for a violation due to reasonable cause and not willful neglect, \$10,000 if due to willful neglect but corrected and \$50,000 if the violation is not corrected appropriately).

Most of the changes to the HIPAA privacy and security provisions will be further detailed in regulations that are yet to be released. Many of the new provisions have unclear effective dates. We will continue to monitor the regulations that are on the horizon in this area and we will be developing a template amendment for business associate agreements.

Please contact the Health Law Group for further information. ■

Contact us if you need additional assistance.

Don B. Weinbren
Tel: 813-223-7474
E-Mail: dweinbren@trenam.com

Richard O. Jacobs
Tel: 727-896-7171
E-Mail: rjacobs@trenam.com

Jacqueline Myles Crain
Tel: 727-896-7171
E-Mail: jcrain@trenam.com

Douglass Farnsworth
Tel: 813-227-7455
E-Mail: dfarnsworth@trenam.com

Michael Igel
Tel: 727-820-3963
E-Mail: migel@trenam.com

TRENAM, KEMKER, SCHARF, BARKIN, FRYE, O’NEILL & MULLIS

TAMPA OFFICE Bank of America Plaza, 101 East Kennedy Boulevard, Suite 2700, Tampa, FL 33602, Phone 813-223-7474
ST. PETERSBURG OFFICE Bank of America Tower, 200 Central Avenue, Suite 1600, St. Petersburg, FL 33701, Phone 727-896-7171

www.trenam.com

The *Trenam Kemker Health Law Update* is a publication of Trenam, Kemker, Scharf, Barkin, Frye, O’Neill & Mullis. All rights are reserved. The information contained in this newsletter is general in nature and is not intended to be, and should not be considered, legal advice. For specific advice on any topic, please call your legal advisor.