Title XIII of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), imposes significant new obligations on "Covered Entities" and "Business Associates" (as defined by HIPAA). Many health care providers, insurers, and health plan administrators may be wondering where to begin. Not only are the potential fines and penalties for violations far higher, but compliance with the new rules requires both Covered Entities and Business Associates to implement precise procedures, provide specific notices, conduct staff training, and draft additional documentation. This legal update summarizes the new privacy and security requirements and suggests practical steps to ensure compliance with the new law.

New Requirements for Covered Entities

Notice of Breach
Effective approximately September 2009

Under the HIPAA privacy rule, Covered Entities are required to "mitigate" the damage caused by a use or disclosure of protected health information ("PHI") that violates their privacy and security policies, but have largely been able to determine how best to do so based on individual circumstances. The HITECH Act will impose more exacting requirements in the event of a "breach." A "breach" is defined by the HITECH Act and includes the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the PHI.

Covered Entities will have a maximum of 60 days from discovery of a breach to notify each individual whose information may have been compromised. The HITECH Act details specific information that must be included in all breach notices. The 60 day clock starts running on the first day that the breach is discovered by any employee or member of the workforce. Therefore, prompt training of employees and staff members is critical to avoid heightened penalties and ensure compliance.
HITECH Act Adds New Requirements to HIPAA for Covered Entities and Business Associates

Covered Entities will face significant public exposure from breaches of PHI. If a Covered Entity's contact information is out of date for ten or more people that are impacted by a breach, it must display a clearly visible notification on its website or send out press releases to broadcast and print media. In addition, for breaches affecting 500 or more people, Covered Entities are required to notify major media outlets and the Secretary of Health and Human Services (HHS) immediately. HHS will also post a list of these 500+ breaches on its website.

**Disclosure Restrictions**
*Effective February 17, 2010*

Under the HITECH Act, individuals will be able to demand stronger disclosure restrictions regarding their PHI. Upon request of an individual, a Covered Entity cannot disclose PHI to a health plan for "payment or health care operations," as defined by HIPAA, if the provider has already been paid in full by the individual for the health care services. Note, disclosures for treatment purposes remain permissible under the previous HIPAA rules.

**Accounting of Disclosures of Electronic Health Records**
*Effective between 2011-2014*

The HITECH Act will require that Covered Entities follow a detailed accounting practice not previously in place under HIPAA. If an individual requests an accounting of electronic health records (EHRs), Covered Entities must be able to provide to the individual disclosure information for the prior three years, if the disclosures were made for "treatment, payment or health care operations."

Covered Entities should start putting in place mechanisms to track such disclosures and revise their Business Associate Agreements to ensure that their Business Associates meet these accounting disclosure requirements as well.

**Prohibition on Sale of EHR or PHI**

**New Marketing Rules**
*Effective approximately February 2011*

The HITECH Act will prohibit the sale of PHI without a valid authorization from an individual in many instances where such sales are now allowed. In addition, many communications which market products or services to individuals will no longer be permissible "health care operation" disclosures.

**New Requirements for Business Associates**
HITECH Act Adds New Requirements to HIPAA for Covered Entities and Business Associates

The HITECH Act makes a major change by directly applying elements of the privacy and security rules to Business Associates. Business Associates must take responsibility for maintaining policies and procedures to ensure full compliance with these rules.

Application of Security and Privacy Rules

Effective February 17, 2010

Business Associates must comply with the following security rules:

- Administrative Safeguards including designating a security official who will be responsible for developing, implementing and evaluating policies to prevent, detect and correct security violations and ensuring that the workforce has appropriate access and training relating to PHI.
- Physical Safeguards to limit physical access to electronic information systems and to address the functionality, accessibility, and movement of workstations utilizing e-PHI.
- Technical Safeguards including limiting the people or software programs who can access e-PHI, putting in place mechanisms to record the activity of systems that contain or use e-PHI, and protecting e-PHI from improper destruction or unauthorized access.

Business Associates who receive PHI under a Business Associate Agreement will be responsible, along with the Covered Entity, for ensuring that Business Associate Agreements satisfy certain HIPAA privacy rules. Business Associates must also take reasonable steps to cure a breach if they know that a Covered Entity is committing a breach. If such steps are unsuccessful, Business Associates must, if feasible, terminate the arrangement or report the problem to HHS.

Notice of Breach, Accounting for Disclosure of EHR, Prohibition on Sale of EHR or PHI & New Marketing Rules

Effective between 2009-2014

As discussed above, Business Associates must notify a Covered Entity within 60 days of discovery of a breach of PHI under the new notice requirements. In addition, the new rules involving accounting for disclosures, sale of EHR, and marketing also apply directly to Business Associates.

Enforcement Provisions

Effective Immediately

The HITECH Act has greatly increased fines and the scope of remedies for violations of HIPAA. These new enforcement provisions apply both to Covered Entities and Business Associates with respect to the current HIPAA rules and regulations today, and the new HITECH Act provisions as each becomes effective. Monetary penalties now range from $100 to $50,000 per individual violation, depending upon the knowledge or intent of
HITECH Act Adds New Requirements to HIPAA for Covered Entities and Business Associates

the person committing the violation. Total penalties per year max out between $25,000 and $1,500,000. The Office of Civil Rights of HHS will retain these funds and use them to further enforce HIPAA and the HITECH Act.

Criminal penalties will be enforced against persons who obtain or disclose PHI without authorization. In addition, a State's Attorney General can bring civil actions against a person on behalf of residents adversely affected by violations of HIPAA or the HITECH Act. The Attorney General can either seek to enjoin further violations or obtain money damages on behalf of the residents harmed. HHS is also beginning to perform periodic audits of Covered Entities and Business Associates to ensure that policies are in place. Finally, individuals harmed by violations will soon be able to recover a percentage of monetary penalties or a monetary settlement. HHS will establish methods for this private recovery in the next three years.

To Do List for Covered Entities and Business Associates

1. Revise existing privacy and security policies and procedures to ensure compliance within the timeframes listed below. Business Associates that do not currently have written policies and procedures must promptly take steps to draft and implement them.

   **Covered Entities & Business Associates**

   Breach Notification Rules - effective approximately September 2009

   Prohibition on Sale of EHR or PHI, New Marketing Rules - effective approximately February 2011

   Accounting of Disclosures of Electronic Health Records - effective between 2011-2014

   Enforcement Provisions - effective immediately

   **Covered Entities**

   Disclosure Restrictions - effective February 17, 2010

   **Business Associates**

   Application of Security and Privacy Rules - effective February 17, 2010

2. Review existing Business Associate Agreements to ensure that the HITECH Act requirements are incorporated.

3. Conduct training for employees and other staff members, focusing specifically on time sensitive issues, such as breach notifications.
HITECH Act Adds New Requirements to HIPAA for Covered Entities and Business Associates

For questions regarding hospitals, physician groups, or other healthcare providers, please contact the Health Law practice group. For questions regarding health plans, please contact the Employee Benefits practice group.