

THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)

WHAT IS IT?

The Health Information Technology for Economic and Clinical Health Act or HITECH Act, expands current federal privacy and security protection for health information. The bill, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) made significant changes to the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA). Numerous HITECH provisions, affecting both covered entities and business associates, become effective as of February 17, 2010.

BACKGROUND

Prior to the passage of HITECH, health care providers, health care plans, and health care data clearinghouses, referred to as covered entities, were solely responsible for complying with HIPAA imposed privacy and security requirements. Service providers with access to the plan's PHI, referred to as business associates, were indirectly regulated through the agreements they had with the covered entities. HITECH changes this by making business associates directly responsible for complying with HIPAA privacy and security rules. HITECH also adds new breach notification requirements for covered entities and business associates, and adds increased penalties for noncompliance.

COVERED ENTITIES

Covered entities should review their existing business associate agreement to ensure they contain the HITECH provisions. Covered entities will want to make sure that the agreement accurately describes the responsibility of both parties regarding the breach notification requirements. Covered entities will also want to confirm that their business associates are now operating in accordance with HIPAA privacy & security.

BUSINESS ASSOCIATES

Under HITECH, HIPAA privacy and security standards now apply directly to business associates. Business associates will now be required to conduct formal risk assessments, appoint a security officer, develop written security policies and procedures, and train employees on how to safeguard protected health information (PHI). Business associates will also be required to protect electronic PHI, through encryption and limited access. Additionally, business associates will now be subject to the same civil and criminal penalties for noncompliance as covered entities. The HIPAA privacy and security provisions, under HITECH, must now be incorporated into business associate agreements.

BREACH NOTIFICATION REQUIREMENTS

HITECH imposes breach notification requirements. Covered entities and business associates otherwise known as HIPAA covered entities that have a breach with respect to unsecured PHI must notify Health and Human Services (HHS) of a PHI privacy or security breach.

A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

- **Notification by a Business Associate**

If a breach of unsecured protected health information, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

- **Individual Notice**

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by e-mail, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach. The notice must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

- **Media Notice**

Covered entities that experience a breach affecting more than 500 residents of a state or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the state or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like the individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- **Notice to the Secretary**

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

DOCUMENTATION

Covered entities and business associates have the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Each improper use of PHI must be investigated to determine if it constitutes a reportable breach. The investigation and determination must be documented. Covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

MINIMUM NECESSARY INFORMATION

Under HIPAA, covered entities must limit PHI to the “minimum necessary” when using or disclosing PHI. HITECH mandates that HHS issue guidance on what constitutes “minimum necessary” by August 17, 2010. Meanwhile, HIPAA covered entities should check their procedures surrounding PHI and limit use and disclosures to the limited data set.

COMPLIANCE STEPS

Even though HITECH's breach notification requirements took effect on September 23, 2009, Health and Human Services (HHS) adopted a non-enforcement policy allowing covered entities and business associates an additional 5 months to comply. The deadline for complying with HITECH requirements is February 17, 2010.

Of immediate concern is to send updated agreements to business associate to make sure they can be executed before February 17, 2010.

Adopt a HIPAA breach notification policy.

Amend HIPAA policies and procedures to address new HITECH requirements.

Train staff on new HITECH procedures.

Conrad Siegel Actuaries Health & Welfare Compliance Committee would be pleased to review HITECH requirements with you and assist in your compliance efforts. Please contact us at hwcompliance@conradsiegel.com.

Our health and welfare compliance updates are designed to provide useful information to organizations about the operation and management of their employee benefit plans. Although we go to great lengths to ensure that only accurate and timely information is provided, we recommend that you consult with an attorney for professional assurance that our information, and your interpretation of it, is appropriate for your particular situation. Nothing provided herein should be construed as legal or tax advice.