



October, 2009

2009-08

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

On February 17, 2009 President Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA), which, among other things, required employers and health plan sponsors to comply with the new COBRA regulations that essentially took effect upon enactment. In addition, ARRA significantly expands the privacy and security standards of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 placing additional responsibilities on “**Covered Entities**” - health plans, health care clearing houses, and health care providers, as well as **Business Associates**, i.e. organizations who perform functions or provide services to the Covered Entities such as administrators, accountants, brokers, and advisors.

This *Insights* will summarize the key HIPAA-related requirements of ARRA contained in the portion of the legislation known as **The Health Information Technology For Economic And Clinical Health Act (HITECH)**. HITECH generally applies as of **February 17, 2010 with certain provisions requiring earlier compliance and others taking effect upon the issuance of applicable regulations.**

What Are The Pre-ARRA HIPAA Privacy and Security Rules?

The HIPAA **privacy rule**, which applies to electronic, paper, and oral transmission of health information, was enacted to help ensure a person’s medical records remain confidential. Fully insured and self insured health plans subject to the privacy rule include medical, dental, vision, prescription drug, health flexible spending account, and long-term care plans as well as some employee assistance plans (EAPs).

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

An employer who sponsors a group health plan, while technically not considered a Covered Entity, is subject to the privacy rule requirements **if any employee has access to Protected Health Information (PHI)**, such as health plan enrollment data. **Protected Health Information** is generally **any information** that

- identifies an individual (such as name, social security number, address), and
- relates to the past, present, or future physical or mental health condition of the individual, or relates to the payment of health care services.

The privacy rule requires Covered Entities (including group health plan sponsors) and Business Associates to:

- Designate a privacy officer who is responsible for developing, implementing and overseeing the plan's privacy policies,
- Create policies and procedures to safeguard the use and disclosure of PHI,
- Create policies and procedures to help protect individual rights with respect to PHI,
- Implement a HIPAA complaint process when an individual believes the confidentiality of PHI has been compromised,
- Train employees about critical privacy practices, and
- Provide a notice of the group health plan's privacy practices to each employee upon enrollment and to issue a reminder notice at least once every three years.

A fully-insured plan that does **not create or receive protected health information** will generally be relieved of the privacy rule requirements. For example, if the employer only receives summary health information (information that summarizes claims history, claims expenses, or types of claims experience of the individuals covered by the plan that is **stripped of all individual identifiers** other than zip codes) or **is made aware** that a participant has enrolled or disenrolled in the plan, the privacy rule will not apply.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

The HIPAA **security rule** is designed to safeguard PHI that is stored or transmitted using electronic media. The security rule requires Covered Entities to establish administrative, technical, and physical safeguards to protect the **electronic** transmission and maintenance of Protected Health Information.

Finally, health records that have been de-identified in accordance with HIPAA standards (all information that can possibly identify the individual has been removed from the record) are not considered PHI and therefore, not subject to HIPAA privacy and security rules.

New Higher Standards For Business Associates

Prior to ARRA, Business Associates were not directly covered by the HIPAA regulations, but instead, were accountable to the Covered Entity only under the terms of the contractual arrangement or Business Associate Agreement (BAA) established between the parties.

Effective February 17, 2010 certain HIPAA security and privacy provisions will now directly apply to Business Associates who, as a result must:

- Establish administrative safeguards to protect electronic PHI,
- Implement physical and technical safeguards (such as locking computers and encrypting email) to limit access and protect the systems that control electronic PHI,
- Update and create security policies and procedures and maintain the necessary documentation,
- Conduct a security risk assessment,
- Appoint a security officer,
- Train employees about how to safeguard the privacy and security of PHI (electronic and paper), and
- Ensure that PHI is not used or disclosed in violation of the terms of the BAA.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

HITECH requires BAAs to include the updated security and privacy changes. While it seems clear that a BAA entered into after February 17, 2010 must contain the new requirements, presently, it is unclear whether existing BAAs need to be restated as the new provisions may be considered incorporated as a matter of law.

The Department of Health & Human Services (HHS) will be responsible to

- Oversee and monitor HIPAA compliance for Covered Entities as well as Business Associates,
- Impose civil and criminal penalties on Covered Entities and Business Associates for HIPAA violations, and
- Issue guidance on methods and technologies to be used to protect PHI.

In April 2009, HHS, as directed, issued initial technology guidance. While not required, using the HHS recommended methods and technologies (such as certain encryption and destruction techniques) to protect PHI creates a safe harbor that will exempt Business Associates and Covered Entities from the new notification requirements in the event a breach is discovered. Annual guidance and updates from HHS will be required.

Breach Notification Requirements

Prior to ARRA, Covered Entities and Business Associates were not obligated under Federal law to notify individuals if a privacy or security breach of PHI occurred. HITECH incorporates very detailed and onerous notification requirements if a “**breach**” of “**unsecured PHI**” is discovered” and recently issued regulations clarified the meaning of these key terms. A **breach**, as originally defined is the “unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information”. The regulations further provide that:

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

- PHI will be considered compromised only if it poses a significant risk of financial, reputational, or other harm to the individual. Covered Entities will be required to perform and document a risk assessment in order to determine if significant harm has transpired.
- “Unauthorized” use and disclosure of PHI means that information was used or disclosed in a manner that is not allowed under the HIPAA privacy rules.
- If PHI is unintentionally accessed or inadvertently disclosed, under certain circumstances, a breach will not be created.

Unsecured PHI is “not secured through the use of a technology or methodology (specified by HHS) that renders the PHI unusable, unreadable or indecipherable to unauthorized individuals.” Regulations make it clear that unless the data is encrypted using HHS standards or completely destroyed, any breach of such information will trigger the notice requirement.

On August 24, 2009 HHS published interim final regulations, and as required by law, the breach notification requirements will become effective on September 23, 2009; 30 days after the regulations were issued. However, HHS recognizes that the 30-day compliance requirement may not allow Covered Entities and Business Associates to properly establish the necessary breach notification processes and procedures. As a result, the regulations provide some relief and HHS will not impose sanctions for failure to provide notifications for breaches that are discovered within 180 days of the release of the regulations (August 24, 2009 - February 22, 2010).

When a breach is discovered, HITECH requires the Covered Entity to issue a written notice to each affected individual by first class mail (or electronic mail if allowed by the individual) without “unreasonable delay” but no later than 60 calendar days after discovery. A breach is generally considered “discovered” when one employee (other than the individual who committed the breach) becomes aware of the violation. If the breach creates the potential for

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

immediate misuse of information, the Covered Entity may be required to notify individuals by telephone or other similar means. The regulations further state that a substitute form of notification is required if the original notice is returned or contact information is insufficient or out-of-date. The manner in which the substitute notice must be delivered depends on how many individuals are affected (more or less than 10 individuals). Business Associates who discover a breach are responsible to notify the Covered Entity and identify each member whose PHI was compromised.

HHS must be notified about all security breaches. If a breach involves more than 500 individuals, HHS must be notified within 60 days of discovery to post the breach information on their website. Covered Entities are also required to maintain a security log and report breaches involving less than 500 individuals to HHS every year no later than 60 days after the end of the calendar year. For 2009, records are only required for breaches that occur after September 23, 2009. Finally, if a breach involves more than 500 individuals in a single state, prominent local media must also be contacted.

Breach notices must be written in plain language and contain the following information:

- A brief description of the event including the date of the breach and the discovery date,
- The types of unsecured PHI that were involved (e.g. Social Security Number, etc.)
- What steps individuals can take to protect themselves,
- A description of the actions being taken by the Covered Entity to investigate the incident, mitigate the losses and to protect against further breaches, and
- Contact procedures for individuals to ask questions or seek additional information.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

Increased Enforcement and Stiffer Penalties

Prior to ARRA, HIPAA enforcement was generally the result of individual complaints. HITECH clearly will change the enforcement landscape and many believe civil and possibly criminal actions will become more commonplace. Major changes and the effective date of these changes are as follows:

As of the Date of Enactment – February 17, 2009

- State Attorneys General have the authority to bring civil actions after notifying the Secretary of HHS.
- Higher monetary penalties may be imposed under a new 4-tier civil penalty structure.

One Year After Enactment – February 17, 2010

- Business Associates will be directly accountable to HHS for failure to comply with the privacy and security rules.
- Covered Entities and Business Associates are subject to required periodic audits.

Two Years After Enactment – February 17, 2011

- HHS must formally investigate when preliminary findings indicate there is evidence of willful neglect, and
- HHS is required by law to impose a civil monetary penalty should the violation be proven to result from willful neglect.

Upon Issuance of Regulations But No Later Than February 17, 2012

- Individuals harmed by the violation can receive a percentage of the penalty or monetary settlement.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

The following table summarizes the HIPAA penalties for privacy and security violations

Type of Violation Based on Degree of Culpability	HIPAA Penalty Based on Nature & Extent of Violation & Harm
Person did not know (or by exercising reasonable diligence would not have known) of the violation (Mitigate penalties if corrected within 30 days)	<ul style="list-style-type: none"> • Minimum \$100 per violation up to \$25,000 per calendar year for identical violations • Maximum \$50,000 per violation up to \$1,500,000 per calendar year for identical violations
Violation Due To Reasonable Cause (Mitigate penalties if corrected within 30 days)	<ul style="list-style-type: none"> • Minimum \$1,000 per violation up to \$100,000 per calendar year for identical violations • Maximum \$50,000 per violation up to \$1,500,000 per calendar year for identical violations
Violation Due To Willful Neglect (and corrected)	<ul style="list-style-type: none"> • Minimum \$10,000 per violation up to \$250,000 per calendar year for identical violations • Maximum \$50,000 per violation up to \$1,500,000 per calendar year for identical violations
Violation Due To Willful Neglect (and not corrected)	<ul style="list-style-type: none"> • 50,000 per violation up to \$1,500,000 per calendar year for identical violations

Expansion of Individual Rights

HITECH gives individual plan participants greater control over the use and disclosure of PHI. Currently, while a participant can request a health plan to restrict the use and disclosure of PHI to carry out treatment, payment and plan operation, the Covered Entity is not bound by the request. Beginning **February 17, 2010** a Covered Entity and their Business Associates must respect the request if:

- The disclosure to the health plan is to carry out payment or operations (not treatment), and
- The PHI relates solely to a product or service which has been entirely paid for by the participant.

Plan participants may request an accounting of their PHI disclosures during a six-year period. However, disclosures relative to the payment, treatment and operation of the plan are specifically exempted from this requirement. ARRA will require that Covered Entities (and possibly their Business Associates) using **Electronic Health Records (EHRs)** for PHI include disclosures for payment, treatment and healthcare operations, but the look back period is limited to three years. Appropriate accounting reports must be submitted to HHS. Due to the administrative complexities, implementation will be predicated upon the issuance of

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

regulations by HHS. The necessary guidance and requirement for compliance is expected between **January 1, 2011 and January 1, 2014.**

Next Steps For Plan Sponsors and Business Associates

HITECH has created new administrative and compliance challenges for plan sponsors as well as Covered Entities and Business Associates. Plan sponsors should review all HIPAA-related policies and practices in order to assure continued HIPAA compliance. Following are action steps plan sponsors can take to prepare for the February 17, 2010 effective date:

- Review and list all plans that are subject to HIPAA.
- Identify all Business Associates such as administrators, brokers, and advisors who perform services to the plans and may come in contact with PHI.
- Contact all Business Associates and confirm that they will be in compliance with new regulations.
- Modify current Business Associate Agreements to incorporate the new privacy and security obligations, as necessary.
- Review and update the designated privacy officer roles and responsibilities as necessary.
- Identify and review current HIPAA policies and procedures such as the collection, storage, and transmission of PHI, forms, breach and incident logs, as well as employee training procedures and materials.
- Train staff about updated HIPAA policies and procedures.
- Develop a breach notification procedure.
- Update the Notice of Privacy practices and distribute updated notices to plan participants.
Note - Privacy Notices for fully insured plans will continue to be the responsibility of and issued by the insurance company or HMO.

Contact your Chernoff Diamond consultant for more information.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

This brief summary is not intended to be a comprehensive legislative analysis. Chernoff Diamond is a benefits advisory firm and does not provide tax or legal advice. Employers should consult with qualified legal and/or tax counsel for guidance in respect of matters of law, tax and related regulation