CONNER STRONG

Legislative Update

May 11, 2009

HIPAA RULE CHANGES WITHIN THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009

Introduction: The American Recovery and Reinvestment Act of 2009 (ARRA) contains funding for Health Information Technology (HIT) and major changes to the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. The HIT is intended to incent health care providers to implement and use electronic health records. Most of the changes from the ACT will take place one year after the enactment, February 17, 2009, but notification regarding security breaches of private health information (PHI) will take effect later this year.

Covered Entities and Business Associates: Currently HIPAA Privacy and Security Rules only applied to "Covered Entities." Covered Entities are defined as health plans, health care providers, and healthcare clearing houses. Covered Entities usually require Business Associates' agreements with third parties, which will require compliance with certain requirements of HIPAA. However, Business Associates are not directly regulated. The ARRA change will apply the same HIPAA standards to Business Associates including any applicable penalties for violations.

Business Associates' agreements will need to be revised to include the new applicable regulations, penalties and notification requirements should a breach of PHI occur and action to cure the breach. If the Business Associate is unsuccessful in complying; then the agreement must be terminated or a notification must be sent to the Secretary of Health and Human Services (HHS).

The Act also requires that the HHS issue guidance on the most effective and appropriate technical safeguards for use in complying with the HIPAA Security Rule. The HHS must issue this guidance annually.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) also expands the Business Associate to include organizations that provide data transmissions of PHI of a Covered Entity to a Business Associate as well as those parties that require routine access to PHI. The change also includes Vendors contracted with Covered Entities to offer Personal Heath Records to patients.

Security Breach Notification: Currently, Covered Entities do not have a specific obligation to report breaches of privacy or security of PHI. The HITECH Act will now require notification to individuals whose "unsecured" PHI has been breached. The HHS is to provide guidance within 60-days of the Act's enactment on technologies considered secure. Should the HHS fail to provide the guidance within the 60-day timeframe then PHI that is secured by a technology standard that makes the PHI unusable, unreadable or indecipherable to unauthorized individuals will be the default. If the breach involved a Business Associate, the Business Associate must notify the Covered Entity. Notification to the individuals must be made without "unreasonable" delay and no later than 60 days after the breach is discovered. The notification should be sent first-class mail though email is permitted if the individual requested such notices be sent electronically.

Should the breach involve more than 500 individuals in a state or jurisdiction then "prominent media outlets" must be notified. Covered Entities must notify the HHS of all breaches on an annual basis but immediately if the breach involves more than 500 individuals. The HHS will post breaches of more than 500 individuals on their website (www.hhs.gov).

The notification must include the following information:

- A description of the breach
- The discovery date of the breach
- The PHI that was breached (i.e. Full Name, Social Security Number, Birth Date, etc.)
- Action the individual should take to protect themselves from possible damage as a result of the breach
- Action the Covered Entity is taking for investigation of incident, to alleviate losses, and safeguards against future breaches
- Advice to the procedure and contact information for individual to obtain additional information, questions. The contact information should include a toll-free number, email address, or website. US Postal mail is also acceptable.

The HHS is required to issue interim final regulations regarding the notification requirements for breaches within 180 days of the enactment. The notification requirement will apply to breaches that are discovered on or after the date that is 30-days after the regulation is issued.

The Act also imposes a temporary breach notification requirement on PHR vendors. These vendors must notify any individual who is a citizen or resident t of the United States of acquired PHR by an unauthorized person because of a breach of security. PHR vendors must notify the Federal Trade Commission (FTC). The FTC will notify the HHS of this breach.

Disclosure Accounting for Individuals: Upon request, an individual has the right to an accounting of disclosures of their PHI. Currently routine disclosures for treatment, payment, or health care operation can be excluded from this accounting. The new law would require disclosures of electronic health records for treatment, payment, or health care operations, if the Covered Entity maintains an "electronic health record" for the individual. These electronic health records disclosures are limited to the 3-year period prior to the request. An electronic health record is defined as an electronic record of health-related information on an individual that is created, compiled, managed, or reviewed by authorized health care clinicians and staff.

The effective date for this provision correlates to the date the Covered Entity maintained the record. For records maintained by a Covered Entity as of January 1, 2009, the disclosure accounting requirement would apply to disclosures on or after January 1, 2014. For electronic health records maintained after January 1, 2009, the requirements apply on or after January 1, 2011 or the date the electronic health record is obtained, whichever is later. These dates may be delayed to 2016 and 2013 respectively.

An individual is permitted to access PHI in an electronic health record in electronic form. The Covered Entity may charge the individual for the cost for providing access. An individual may also direct the Covered Entity to transmit the electronic health records directly to another person or entity. This provision is effective on February 17, 2010.

Right to Restrict Disclosure of Individual's PHI: Currently the Covered Entity may disclose PHI for treatment, payment, or health care operations even if the individual requests that the PHI be not disclosed. The HITECH Act will require Covered Entities to comply with the individual's request to restrict disclosures to a health plan for payment or healthcare operations if the PHI pertains to services or treatment that have been paid out of pocket and in full. This provision is effective on February 17, 2010.

Restrictions on Disclosures: The HITECH Act imposes several new restrictions on PHI disclosure:

Prohibits the Sale of PHI – Covered Entities and Business Associates may not receive compensation for the PHI disclosure without the individual's authorization. Payment for research purposes is limited to the cost of preparing and transmitting the data. HHS is required to issue regulations implementing the new restrictions within 18 months. The new rule will become effective after 6-months of regulation issuance.

- *Restricts marketing communications* – Covered Entities and Business Associates will no longer be allowed to market to an individual information on products or services without the individual's authorization if the Covered Entity or Business Associate receives compensation from a third-party for the communication. This new rule excludes communication about a drug the individual is already taking and where compensation

for the communication is reasonable or where the communication is made by a Business Associate on behalf of the Covered Entity and is consistent with the terms of the business associate agreement.

- *Imposes "minimum necessary" limits* – The HITECH Act requires HHS to issue regulations within 18 months on what constitutes the "minim amount necessary." Until the guidance is issued, Covered Entities must use or disclose limited data set that is sufficient to complete the intended purpose. A limited data set excludes certain identifying information but is not fully-deidentified.

Civil Penalties: Under the Act, HHS will be required to perform periodic audits of Covered Entities to ensure compliance. The HITECH Act increases the amounts of penalties that differentiate between types of violations. Penalties may be waived if the violation is corrected within 30-days of the date the violation was discovered. HHS will be required to assess penalties for violation of willful neglect and to investigate complaints of violations.

VIOLATION CLASSIFICATION AFTER FEBRUARY 17, 2009	MINIMUM PENALTY	MAXIMUM PENALTY PER CALENDAR YEAR
Individual does not know of the violation	$100 per violation	$25,000 for the same violations
Reasonable cause	$1,000 per violation	$100,000
Corrected violation caused by willful neglect	$10,000 per violation	$250,000
Any violation or caused by willful neglect and not corrected	$50,000	$1.5 million

Additional enforcement provisions apply to penalties imposed 24 months after the date of enactment. The HHS is required to issue regulations governing the enforcement provision within 18 months to enactment. The Act requires the General Accounting Office to review methodologies for allowing a portion of civil penalties to be paid to affected individuals. This methodology must be established by February 17, 2012.

The Act authorizes State Attorney General to initiate civil actions against Covered Entities to enjoin further violations and seek damages on behalf of their state residents if the HHS has not taken action. The amount of damages is up to $100 per violation with a maximum of $25,000 per calendar year for identical violations. This provision is effective for any violation occurring after February 17, 2009.

Criminal Penalties: The Act does not change current criminal penalties that may be imposed.

VIOLATION CLASSIFICATION	FINES	PRISON
Knowing violations	$50,000	One year
Committed under false pretenses	$100,000	Five years
Committed for commercial or personal gain	$250,000	Ten years

Action Steps toward Compliance

Many provisions outlined in the new laws require additional guidance, and the HHS is expected to issue interim final regulations by August 16, 2009. These regulations will apply to breaches 30 days after the date of the publication. While the upcoming months are expected to bring clarity and many are awaiting the additional guidance to fully understand compliance obligations, employer s may consider the following regarding steps toward compliance.

- By August 2009, HHS will regionally designate offices to offer guidance, assistance and education regarding privacy and security rights and responsibilities to covered entities, business associates, and individuals. For additional information regarding these future session, visit the HHS website at: www.HHS.gov
- By February 2010, HHS will conduct education initiatives regarding acceptable uses of PHI. Covered entities and Business Associates are strongly urged to attend such training initiatives.
- Business Associate agreements will need to be reviewed and revised to address the new stipulations ARRA imposes on Covered Entities and Business Associates.
- Current HIPPA polices and administrative practices should be evaluated to incorporate the new requirements as they relate to security breaches in PHI, an individuals right to request and restrict disclosures of PHI, and the HITECH Act's restrictions on PHI. While many provisions have future effective dates, plan administrators may want to begin to examine how these new laws will be addressed and implemented.

Please contact your Conner Strong representative with any questions, toll-free at 1-877-861-3220.