



## EMPLOYEE BENEFITS LAW **ALERT**

March 19, 2009

### HIPAA Changes Affecting Group Health Plans And Business Associates Made By The American Recovery And Reinvestment Act Of 2009

In addition to the COBRA subsidy, the American Recovery and Reinvestment Act of 2009 (“ARRA”), enacted on February 17, 2009, made significant changes to HIPAA privacy and security obligations. Those changes affect covered entities, including group health plans, and also affect business associates. Although most of the HIPAA changes are effective February 17, 2010, one change (regarding breach notifications) will become effective earlier. A summary of the key provisions affecting group health plan covered entities and business associates is below.

- **Requirement to Notify Individuals of HIPAA Breaches.** The law changes now require covered entities to notify each individual whose unsecured protected health information (“PHI”) has been breached. For a breach of PHI under the control of a business associate, the business associate is required to notify the covered entity. Notice of the breach has to be provided to the Secretary of the US Department of Health and Human Services (“HHS”) and in the case of a mass breach involving more than 500 individuals, to a prominent media outlet. Unsecured PHI means PHI that is not secured through the use of a technology or methodology specified by the Secretary of the US Department of Health and Human Services.

The Secretary of HHS is required to issue guidance about acceptable technology within 60 days of February 17, 2009. The law contains a default description of acceptable technology in the event that HHS does not timely issue guidance. ***The ARRA directs the HHS to issue regulations within 180 days of February 17, 2009. Then, the new notification requirements will apply to breaches discovered on or after the date that is 30 days after the date the regulations are published.***

- **Additional Individual Rights.**
  - Accounting of Disclosures for Treatment, Payment and Health Care Operations. Under current law, individuals have the right to an accounting of disclosures of their PHI made in the previous six (6) years requiring covered entities to track the disclosures. There are certain exceptions to the accounting requirement such as disclosures that are made for treatment, payment, or health care operations. Now, a covered entity that uses or maintains an “electronic health record” with respect to PHI must account for disclosures for treatment, payment, and health care operations. This accounting is limited to disclosures made in the previous three (3) years. HHS is required to promulgate regulations implementing this new requirement.

***There are two general effective dates:*** (1) with respect to electronic health records acquired by a covered entity on January 1, 2009, the effective date is January 1, 2014 and

(2) with respect to electronic records acquired by a covered entity after January 1, 2009, the effective date is January 1, 2011 or, if later, the date the electronic record is acquired.

- Access to PHI in Electronic Form. If a covered entity uses or maintains an electronic health record for PHI, the new law gives individuals the right to obtain a copy of the PHI in electronic format. The individual can also direct the covered entity to transmit an electronic copy directly to an entity or person designated by the individual. ***This requirement is effective as of February 17, 2010.***
- Right to Restrict Disclosures for Payment & Health Care Operations. Under current law, individuals have the right to request that a covered entity not disclose their PHI for purposes of routine treatment, payment, or health care operations, although the covered entity is not required to agree to the restriction. Now, the covered entity must agree to the restriction for purposes of payment and health care operations (but not for purposes of treatment) if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full. ***This requirement is effective as of February 17, 2010.***

- **Changes Involving Business Associates.**

- Direct Application of Rules to Business Associates. Under existing law, HIPAA applies to covered entities directly and only indirectly to business associates via business associate contracts. With the law changes, business associates are directly and expressly subject to the same physical, technical and administrative safeguards and policies and procedures requirements as covered entities for purposes of the security rule. This means that business associates of covered entities will need to take specific actions to conform their operations to these requirements including, for example, appointing a security official, conducting a risk assessment, developing written policies and procedures, implementing appropriate physical and technical precautions (such as locking computers or email encryption) to protect electronic PHI and to train its workforce on protection of electronic PHI. The Act also indicates that the additional security requirements applicable to covered entities (presumably the new AARA requirements ) also apply to business associates and must be incorporated into business associate agreements.

The new provisions directly govern business associates for privacy purposes by allowing use and disclosure of PHI only if the use or disclosure is in compliance with privacy standards articulated in the privacy regulations (specifically those regulatory standards that today are required to be incorporated in business associate contracts). The law also indicates that the additional privacy requirements applicable to covered entities (presumably the new AARA requirements) are also applicable to business associates and must be incorporated into business associate contracts.

- Civil and Criminal Penalties. Business Associates are directly subject to civil and criminal penalties for violations of their obligations to the same extent as covered entities.
- Effective Date. The business associate changes are ***effective February 17, 2010.***

- **Enforcement Changes.**

- Civil Penalties. Civil monetary penalties are significantly increased consisting of a tiered structure with penalties ranging from \$ 100 with a \$25,000 cap for identical violations per

calendar year, to \$50,000 per violation with a cap of \$1, 500,000 per year for identical violations.

- Criminal Penalties. The law clarifies that criminal penalties can apply to employees and others who wrongfully obtain or disclose PHI held by a covered entity.
- Enforcement by Attorneys General. State attorneys general may bring civil suits against individuals who violate privacy and security standards.
- Effective Date. The changes to the enforcement provisions became ***effective as of the date of enactment, which was February 17, 2009.***
- **What Needs to Be Done.**
  - Group Health Plans. By February 17, 2010, sponsors, administrators, and/or group health plans should:
    - revise HIPAA policies and procedures and notice of privacy practices and develop breach notification procedures to conform with the new rules;
    - update existing and new business contracts to incorporate the new rules;
    - review HIPAA plan amendments to determine whether any updates are necessary as a result of the new rules;
    - train the workforce on the new rules; and
    - review insurance policies to determine whether there is coverage in connection with HIPAA failures and if so whether that coverage is adequate given the increased civil penalties.
  - Business Associates. Business associates of covered entities will need to conform their operations to comply with their new direct security and privacy obligations by February 17, 2010.

If you have any questions, please contact Joni Landy at 412.594.3945 (or [jlandy@tuckerlaw.com](mailto:jlandy@tuckerlaw.com)), David Sawyer at 412.594.5642 ([dsawyer@tuckerlaw.com](mailto:dsawyer@tuckerlaw.com)), or any Tucker lawyer with whom you regularly work.

\*\*\*\*\*

*Employee Benefits Law Group: The Employee Benefits Law Group at Tucker Arensberg, P.C. has a diverse client base of private and public employers. We are dedicated to working with our clients to resolve complicated legal issues in a practical, common-sense and cost-efficient manner. In doing so, we routinely work with our clients to design, establish, implement, administer, and terminate many different types of employee benefit plans. Refer to <http://www.tuckerlaw.com/practice/employee.html> for more information on the Employee Benefits Law Group.*

*TAX ADVICE DISCLAIMER: Any federal tax advice contained in this communication (including attachments) was not intended or written to be used, and it cannot be used, by you for the purpose of (1) avoiding any penalty that may be imposed by the Internal Revenue Service or (2) promoting, marketing or recommending to another party any transaction or matter addressed herein. If you would like such advice, please contact us.*