Health Care Alert

SUMMARY OF CHANGES TO HIPAA PRIVACY AND SECURITY REQUIREMENTS INCLUDED IN THE AMERICAN RECOVERY AND REINVESTMENT ACT

MVA Health Care Team

04.2009

Business Associates Notification Accountings Marketing Other Changes

On February 17, 2009, the American Recovery and Reinvestment Act (the "Act") was signed into law. A portion of the Act, known as the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), relates to investments in health information technology. To address concerns about the security and privacy of medical information as the use of health IT increases, the HITECH Act contains a number of changes to HIPAA's Privacy and Security Rule requirements. This alert is intended to provide a brief overview of some of these changes made to HIPAA.

Many details regarding these new requirements are not known. The HITECH Act directs the Secretary of DHHS (the "Secretary") to issue further regulations on certain specific matters addressed in the HITECH Act and to revise the current regulations issued with respect to HIPAA's privacy and security requirements to make them consistent with the HITECH Act.

Application of Security Rule to business associates

One of the most significant changes to HIPAA made in the HITECH Act is the extension of the Security Rule's administrative, technical and physical safeguard requirements to business associates. These new requirements, including development of privacy and security policies and procedures by the business associate, must be incorporated into the business associate agreement between the covered entity and the business associate. Additionally, the HITECH Act requires the Secretary to issue guidance on an annual basis on the "most effective and appropriate technical safeguards" and subjects business associates directly to penalties for violations of the Security Rule's requirements. This requirement is effective February 17, 2010.

Notification requirements in case of breach of PHI

Upon discovery of a breach of "unsecured protected health information", covered entities must notify each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired or disclosed. The HITECH Act defines "unsecured protected health information" as PHI that is not secured through the use of a technology or methodology specified by the Secretary in regulations as rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. On April 17, 2009, the Secretary issued guidance regarding the use of encryption and destruction to secure information.

If more than 500 individuals are involved in the breach, the covered entity must notify the Secretary and prominent media outlets in the state or jurisdiction in which the affected individuals live. The HITECH Act provides information on the timeframes for, and content of, the notice. Covered entities will also be required to maintain a log of all breaches and submit it to the Secretary on an annual basis.

The HITECH Act requires the Secretary and the Federal Trade Commission to issue interim final regulations within 180 days after the enactment of the Act (August 16, 2009) with respect to the notification requirements, and then they will become effective for breaches discovered on or after 30 days from the date of the publication of the interim final regulations. Therefore, the requirements will go into effect no later than September 15, 2009.

Accounting of disclosures

Currently, the Privacy Rule grants individuals the right to receive an accounting of disclosures made during the previous six years, certain kinds of disclosures do not have to be included in the accounting, including disclosures made for treatment, payment or health care operations. The HITECH Act will require covered entities that use electronic health records (EHRs) to include information regarding disclosures for treatment, payment and health care operations during the three years prior to the request in the accounting of disclosures. For covered entities that do not currently use EHRs, this new requirement will apply on the later of January 1, 2011 or the date the entity begins to use EHRs. Regulations will be issued regarding the information to be collected on these disclosures.

Marketing and fundraising uses

Under the HITECH Act, marketing communications will be restricted if the covered entity will receive direct or indirect payment in exchange for making the communication. The Act creates exceptions to the restriction in three instances: (1) the communication describes a drug or biologic currently being prescribed for the recipient of the communication and the payment to the covered entity is "reasonable in amount" (to be defined in a regulation); (2) the communication is made by the covered entity and the individual has given his/ her authorization to the communication; and (3) the communication is made by a business associate of the covered entity and is consistent with a written agreement between the business associate and the covered entity. In addition, all fundraising communications must contain an opportunity for the recipient to opt out of further future communications. These changes will be effective February 17, 2010.

Other Changes

A few other changes to the Privacy and Security Requirements include:

- **Requested restrictions.** Covered entities must comply with requests from individuals to restrict disclosures of PHI to health plans for the purposes of carrying out payment or health care operations if the PHI pertains solely to a health care item or service for which the provider has been paid out of pocket in full.
- **Minimum necessary.** HIPAA's Privacy Rule requires covered entities to disclose the minimum necessary PHI to accomplish the intended purpose of the disclosure, use or request. The Act directs the Secretary to issue

guidance on the meaning of "minimum necessary" no later than July 17, 2010.

- **Prohibition of sale of PHI.** The Act mandates that covered entities may not—directly or indirectly—receive remuneration in exchange for any individual's PHI unless the individual gave the covered entity an authorization specifically stating that PHI can be further exchanged for remuneration.
- **Access to information in electronic format.** Covered entities that use or maintain EHRs must permit individuals to receive an electronic copy of their PHI and to direct the covered entity to send the information directly to another entity or individual.
- **Civil actions for HIPAA violations.** Effective immediately, the Act authorizes each State Attorney General (AG) to pursue civil actions for HIPAA violations that have threatened or adversely affected a resident of the AG's state.
- **Mandatory compliance audits; increased penalties.** The Act directs the Secretary to conduct periodic audits of covered entities and business associates regarding compliance with the Privacy and Security Rule and increases civil monetary penalties for HIPAA violations. The increases in the amount of penalties are effective immediately, except that the regulations related to willful neglect will not be effective until February 17, 2011.