Legal Alert: Economic Stimulus Act Impacts HIPAA Requirements

2/23/2009

The American Recovery and Reinvestment Act ("ARRA") signed into law on February 17, 2009 includes significant changes to the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA). Below are highlights of some of the significant changes and their effective dates.

Application of Privacy and Security Rules to Business Associates: The ARRA will make the HIPAA privacy and security rules, which currently only apply to covered entities (defined as health plans, health care providers, and health care clearinghouses), applicable to business associates of covered entities. A HIPAA "business associate" is any person or entity who, on behalf of a covered entity, performs or helps perform a function or activity involving the use or disclosure of protected health information. While business associates are not directly subject to HIPAA, they may be indirectly regulated by HIPAA through the business associate agreements covered entities must establish with them

However, effective 12 months after the enactment of ARRA, the privacy and security rules under HIPAA and its civil and criminal penalties will apply to business associates in the same way it applies to covered entities. All business associate agreements will need to be updated to comply with the changes under ARRA on or before February 17, 2010.

Notification of Security Breaches: In the event of a breach of unsecured protected health information, ARRA imposes certain notification requirements on covered entities and business associates. Unsecured protected health information is defined as protected health information that is not secured using Secretary of Health and Human Services-approved standards. The covered entity or business associate must provide notification of a breach of unsecured PHI "without unreasonable delay", and in no case later than 60 days, after discovery of the breach. A business associate who discovers a breach must report it to the covered entity. In the case of a breach discovered by the covered entity, the notice is to be provided directly to the individual impacted or to prominent media outlets of a state or jurisdiction if 500 or more residents are impacted. Additionally, for a breach involving 500 or more individuals, notice must be provided immediately to the Secretary of Health and Human Services.

The notification of breach must include the following information (to the extent possible):

• A brief description of what happened, including the date of the breach and

the date of the discovery of the breach, if known.

• A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).

• The steps individuals should take to protect themselves from potential harm resulting from the breach.

• A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

• Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

The ARRA directs the Secretary of Health and Human Services to promulgate interim final regulations no later than 180 days after the enactment date of the ARRA. The notification duty provisions of the ARRA apply to breaches that are discovered on or after the date that is 30 days after the date of publication of such interim final regulations.

Civil Penalties and Enforcement: The new law expands the existing civil penalties and enforcement provisions which are effective for all violations after the date of enactment of ARRA. The civil penalties are increased and categorized by type as follows:

• **Tier 1** – Where the person is unaware of the violation, and would not have known even with reasonable diligence, the penalty is at least $100 per violation not to exceed $25,000 for all violations of the same requirement during the year.

• **Tier 2** – Where the violation is due to "reasonable cause" and not willful neglect, the penalty is at least $1,000 per violation not to exceed $100,000 for all violations of the same requirement during the year.

• **Tier 3** – Where the violation is due to willful neglect but is corrected within 30 days, the penalty is at least $10,000 per violation not to exceed $250,000 for all violations of the same requirement during the year.

• **Tier 4** – Where the violation is due to willful neglect and is not corrected within 30 days, the penalty is at least $50,000 per violation not to exceed $1,500,000 for all violations of the same requirement during the year.

ARRA also expands its enforcement provisions by providing state Attorneys General with authority to bring civil actions in federal court against any person whose violations pose a threat to or harms one or more residents of the state. Such actions may be sought to enjoin such violations or obtain damages of up to $100 per violation up to a maximum of $25,000 for all violations of the same requirement during a calendar year.

ARRA made several other changes to HIPAA's privacy and security rules. You should be sure to review all the changes made to ensure compliance with the new provisions. If you have any questions regarding these new requirements, please contact the Ford & Harrison attorney with whom you usually work or any member of Ford & Harrison's Employee Benefits practice

group.