

# Health Law Alert

## Federal Stimulus Law Raises the Bar for Health Information Privacy and Security

The federal stimulus law enacted on February 17, 2009, the “American Recovery and Reinvestment Act of 2009” (ARRA), contains many new compliance challenges for entities who create, maintain, transmit, access, use or market health information. In addition to creating a new federal bureaucracy for a new national electronic health records (EHR) infrastructure to set EHR standards and administer EHR stimulus money, and establishing new Medicare and Medicaid reimbursement methods to incent EHR adoption, ARRA contains many new health information privacy and security requirements.

This Health Law Alert summarizes the most significant privacy and security requirements of Title XIII of ARRA, the “Health Information Technology for Economic and Clinical Health Act” (HITECH). Under HITECH, health care providers and companies currently regulated as HIPAA covered entities will be subject to new privacy and security obligations, and entities which are not currently regulated under HIPAA, including vendors to covered entities, will be directly regulated under these new privacy and security obligations and will be subject to penalties for non-compliance.

### ***New Federal Breach Notification Requirements***

Prior to HITECH, HIPAA covered entities had no statutory or regulatory obligation to notify individuals of breaches of protected health information (PHI) unless required to do so by applicable state breach notification laws. HITECH not only creates a new federal breach notification obligation applicable to HIPAA covered entities but also creates new breach notice obligations applicable to certain entities not currently regulated by HIPAA.

#### ***Breach notice requirements: HIPAA Covered Entities and Business Associates***

No later than 60 days after discovering a breach of unsecured protected health information, a covered entity is required to notify each affected individual that their information has been, or is reasonably believed to have been, accessed, acquired, or disclosed. Under HITECH, a breach occurs when there is an unauthorized acquisition, access, use or disclosure which compromises the security or privacy of PHI. HITECH defines “unsecured protected health information” (unsecured PHI) as protected health information that is not secured through the use of technology or methods to be specified in guidance issued by the HHS Secretary; HITECH directs the HHS Secretary to issue guidance specifying which technologies and methods render PHI unusable, unreadable or indecipherable to unauthorized individuals.

HITECH permits breach notices to be made by written or electronic mail, or by a posting on the covered entity’s web site or in a media outlet if there is insufficient contact information for 10 or more

individuals. If 500 or more individuals’ information is involved, media notice must be provided and the covered entity must also immediately notify the Secretary of Health and Human Services (HHS). HITECH specifies that the content of breach notices must include a description of what happened, the dates of both the breach and the discovery of the breach, a description of the information involved in the breach, the steps that individuals should take to protect themselves from potential harm from the breach and a description of what the covered entity is doing to investigate, mitigate losses and protect against further breaches.

HITECH also establishes a statutory breach notification requirement directly applicable to HIPAA business associates. Under HITECH, a HIPAA business associates is obligated to notify the covered entity of a breach of unsecured PHI. The notice from the business associate to the covered entity must be provided no later than 60 days from the discovery of the breach and must include the identification of each individual impacted by the breach.

#### ***Breach Notice Requirements: Vendors of “Personal Health Records”***

Vendors of personal health records (PHRs) are obligated under HITECH to provide certain notifications in the event of a breach of security. As distinct from an EHR containing PHI created and maintained by a HIPAA covered entity, a PHR is typically initiated and maintained by an individual, often through the services of a PHR vendor, such as a sponsor of an internet-based PHR platform. HITECH’s new definitions key to understanding these new PHR requirements include “personal health record”, “breach of security”, “PHR identifiable health information”, and “unsecured PHR identifiable health information.”

Under HITECH, a “personal health record” is defined as an electronic record of PHR identifiable health information about an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual. “PHR identifiable health information” means individually identifiable health information that is provided by or on behalf of the individual and that identifies the individual or that there is a reasonable basis to believe that the information can be used to identify the individual. “Unsecured PHR identifiable health information” means PHR identifiable information that is not protected through the use of technology or methods as specified in guidance to be issued by the Secretary of HHS (through the same guidance process applicable to unsecured PHI, discussed above). “Breach of security” means, with respect to unsecured PHR identifiable health information in a PHR, acquisition of such information without the authorization of the individual.

Following the discovery by a PHR vendor of a breach of security of unsecured PHR identifiable health information, the PHR vendor must notify each individual impacted and must also notify the Federal Trade Commission (FTC). The same requirements for timing, method and content of breach notices applicable in the HIPAA context for breaches

of unsecured PHI, discussed above, apply to breach notices for unsecured PHR identifiable health information.

### ***Breach notification compliance due after regulations are issued***

HITECH directs the Secretary of HHS to issue regulations implementing HITECH's breach notification requirements applicable to HIPAA covered entities and business associates and directs the FTC to issue regulations implementing the breach notification requirements applicable to vendors of PHR no later than 180 days from the enactment of ARRA. Compliance with the breach notification requirements will be required for breaches discovered 30 days after the regulations are published.

### ***Direct Regulation of HIPAA Business Associates***

In addition to the new breach notification requirements discussed above, HIPAA business associates have other new direct statutory obligations regarding information security and privacy. HITECH mandates that HIPAA's obligations to implement administrative, physical and technical safeguards for electronic PHI and to implement security policies and procedures apply to HIPAA business associates in the same manner as covered entities. Additionally, the privacy and security requirements under HITECH will also apply to business associates, and HITECH directs that such privacy and security requirements be incorporated into business associate agreements with covered entities. It is significant also that HITECH mandates that HIPAA's penalty provisions related to these privacy and security requirements apply to business associates. These new requirements for HIPAA business associates are effective a year from ARRA's enactment.

### ***Accountings of Disclosures Broaden***

Under HIPAA's access provisions, individuals are entitled to receive from covered entities accountings of disclosures of their PHI, however covered entities are not currently required to account for disclosures made for treatment, payment or health care operations purposes. Under HITECH, covered entities will be required to track and account for disclosures made through an EHR for treatment, payment and health care operations. HITECH also mandates an accounting process under which business associates will be obligated under certain circumstances to provide an accounting of disclosures of PHI.

The Secretary of HHS is to issue implementing regulations regarding the specific information that must be collected about each disclosure. The compliance timeframe for these broadened accounting requirements may be impacted by when a covered entity acquires EHRs and whether the Secretary establishes a compliance date by regulation.

### ***Restrictions on Selling PHI and Marketing Communications***

HITECH prohibits HIPAA covered entities and business associates from receiving direct or indirect remuneration in exchange for any PHI, unless a HIPAA-compliant authorization is obtained that includes whether the PHI may be further sold by the receiving entity. Exceptions to the sale of PHI include public health, research or treatment purposes, merger or sale of the covered entity, and service payments to business associates. Compliance with the prohibition on selling PHI is required 6 months from the issuance of implementing regulations.

HITECH also fine-tunes HIPAA's prohibition against using PHI for marketing purposes. HITECH considers impermissible marketing to include using or disclosing PHI for communications for purposes otherwise permissible under HIPAA, such as for treatment or case

management, if the covered entity receives payment, directly or indirectly, for the communication. However, if the communication describes a drug or biologic that is currently being prescribed, the payment to the covered entity is reasonable, the communication is made by the covered entity and the covered entity obtains a HIPAA-compliant authorization, the communication would be permissible as part of the covered entity's health care operations. Also, where the communication is made by a business associate on behalf of a covered entity and is consistent with the written agreement between the covered entity and the business associate, the communication would be permissible.

### ***Enforcement Toughened***

HITECH requires the Secretary of HHS to investigate and impose penalties where violations of HIPAA requirements are due to willful neglect. HITECH also modified the tiered levels of civil monetary penalties for violations of HIPAA privacy and security requirements, depending on levels of knowledge or willfulness, including whether violations were not known and through reasonable diligence could not be known, whether violations are due to reasonable cause, or whether violations are due to willful neglect. The amounts of civil monetary penalties attached to these tiers range from \$100 to \$50,000 per individual violation, subject to annual maximums ranging from \$25,000 to \$1.5 million for total violations of the same requirement.

For the first time, state attorneys general may bring civil actions on behalf of state residents whose interests are threatened or adversely affected by HIPAA violations. In order to bring an action, an attorney general must give prior notice to the Secretary of HHS who has the right to intervene in the action. An attorney general may not bring an action if a federal action has already been instituted.

These enforcement provisions are effectively immediately.

### ***HITECH Privacy and Security: More to Come and Much to Do***

While most of HITECH's provisions require regulatory action in order to implement HITECH's requirements, it is clear that the new law places significant new compliance obligations on health care providers, health plans, business associates and vendors of PHRs. As we anticipate HITECH guidance and regulations, organizations should begin assessing HITECH's impact, including:

- Assessing encryption or other available technology, as may eventually be blessed by HHS, in order to minimize the use of unsecured PHI and unsecured PHR identifiable health information;
- Adding breach notification processes to existing compliance programs;
- Planning a process to amend HIPAA business associate agreements to comply with HITECH's requirements;
- For business associates who will now have direct legal obligations regarding the security and privacy of PHI, understanding and preparing to implement HIPAA's electronic PHI security safeguards and related policy and procedures requirements; and;
- Reviewing existing PHI disclosure tracking and reporting capabilities to ensure that disclosures for treatment, payment and health care operations can be tracked and accounted for.

– Katherine M. Keefe, Esquire

*For questions regarding HITECH or any other health information privacy and security issue, please contact Katherine M. Keefe at (610) 354-8270 or [kmkeefe@mdwccg.com](mailto:kmkeefe@mdwccg.com).*