

Pierce & Mandell, P.C.

Attorneys at Law

11 Beacon Street, Suite 800

Boston, MA 02108-3002

(617) 720-2444 Fax: (617) 720-3693

www.piercemandell.com

HEALTH INFORMATION TECHNOLOGY AND THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009

By: Emily Kretchmer and William Mandell

On February 17, 2009 President Obama signed into law the American Recovery and Reinvestment Act of 2009, the Stimulus Bill. Title XIX of the Stimulus Bill, known as the “Health Information Technology for Economic and Clinical Health Act” or “HITECH Act”, includes broad federal initiatives for the adoption of health information technology and the significant expansions to HIPAA which improve the safeguards for the privacy and security of individual identified health information.

Specifically, the HITECH Act directs approximately \$150 billion in new funds to the healthcare industry over the next two years. The spending includes \$87 billion for Medicaid, \$24.7 billion to subsidize private health insurance for people who have lost their jobs, \$19.2 billion for health information technology and \$10 billion for the National Institutes of Health.

The HITECH Act sets a goal that electronic health records will be used for each person in the United States by 2014. This is an extension of goals already set by many states. In particular, Massachusetts enacted in 2008 an Act to “Promote Cost Containment, Transparency and Efficiency in the Delivery of Quality Health Care” which sets a goal of statewide adoption of electronic health records by the year 2015 to improve patient safety and lower costs. After this date, the use of an interoperable health record system would be required for hospital licensure in the Commonwealth. In 2009 and 2010, Medicare is also offering physicians who successfully e-prescribe a bonus payment of 2 percent of their overall Medicare reimbursement.

The HITECH Act is effective as of February 2010, unless otherwise indicated. In addition, the federal Department of Health and Human Services (“DHHS”) has been tasked to issue regulations with implement HITECH Act which will give the health care industry more guidance on how to implement these provisions.

The major provisions of the HITECH Act related to HIPAA and Electronic Medical Records (“EMRs”) are:

HIPAA

Security of Health Information

- DHHS shall issue annual guidance on the most effective and appropriate technical safeguards and security standards for use in protection health information.

Business Associates

- Business Associates will be subject to stricter compliance standards. Business Associates will be directly responsible for full compliance with the relevant requirements of the Privacy Rule and subject to civil and criminal penalties if they fail to do so.
- Business Associates that obtain or create PHI pursuant to a written business associate agreement may use or disclose the PHI *only* in compliance with the business associate agreement and must report any unauthorized disclosures to the Covered Entity.

Security Breaches of Unsecured PHI

- The breach notification provisions are effective for breaches that occur 30 days after DHHS publishes interim final regulations, which are due within 180 days of enactment of the HITECH Act.
- Unsecured PHI is PHI which is not encrypted.
- In the event there is a security breach of Unsecured PHI that affects less than 500 individuals, Covered Entities must notify the affected individuals within sixty (60) days of the discovery of such breach, absent a law enforcement official's instructions to the contrary. A security breach is deemed discoverable on the first day that the breach is known or should reasonably have been known by the entity, including any employee, officer or "other agent" (other than the individual committing the breach).
- In the event a security breach of PHI affects 500 or more individuals, notice of the breach must be provided immediately to such individuals.
- Covered Entities may maintain a log of breaches involving less than 500 individuals, and provide the log to DHHS annually. DHHS will post on its website a list of Covered Entities providing a notice of breaches involving 500 individuals or more individuals.
- Business Associates must report security breaches to a Covered Entity within the same time frame as above, failure to do so will subject them to direct enforcement and penalties.

Vendors and Service Providers of Personal Health Records ("PHRs")

- Until Congress enacts new legislation establishing requirements for security breach notifications for entities that are not covered under HIPAA, a Personal Health Record Vendor has the same obligations to report security breaches as a Covered Entity and Business Associate as described above.
- In addition, security breaches related to PHRs are initially reported to the Federal Trade Commission ("FTC"). The FTC will notify the Secretary of Health and Human Services.
- Failure of vendors and service providers to comply with reporting requirements constitutes an "unfair and deceptive trade practice" enforceable within the FTC's jurisdiction.

- A PHR is an electronic record of PHI that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual which is held by a PHR vendor or service provider. A third party PHR service provider is an entity that provides services to the vendor in connect with offering or maintenance of a PHR or a related product or service and that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses unsecured PHI which is maintained in a PHR.

Disclosure of Healthcare Expenses Paid Out-of-Pocket by the Individual

- Currently under HIPAA, an individual may request restrictions on the disclosure of his/her PHI; however a Covered Entity has discretion to grant the request but must maintain the request in the individual's health record.
- Under the HITECH Act, a Covered Entity will be required to agree to an individual's request for privacy protections for disclosure of PHI related to payment or healthcare operations if the information pertains only to a healthcare item or service that the individual has paid for out-of-pocket, in-full, unless disclosure is otherwise required by law or is for treatment purposes.
- Limited disclosure of out-of-pocket healthcare expenses is meant to address consumers privacy concerns about Health Care Information Exchanges (HIEs – f/k/a Regional Health Information Networks (RHIOs), because individuals might not want their insurance companies to know about certain treatment that would affect the individual's insurance rates or insurability.

Minimum Necessary

- The HITECH ACT refines the minimum necessary concept of disclosure to mean, to the extent practicable, PHI disclosure should be a limited data set, which does not include any direct identifiers.
- DHHS is directed to issue guidance on what constitutes the minimum necessary within 18 months of HITECH Act's enhancement. This provision will sunset after those regulations are issued.

Accounting of Disclosures

- Covered Entities which use EHRs must provide individuals, upon request, with an accounting of disclosures of their PHI, including disclosures made for treatment, payment or healthcare operations.
- For disclosures by a Business Associated, the Covered Entity may provide the accounting or direct the individual to the Business Associates, who must comply with the accounting requirements.
- The accounting period is limited to three (3) years.

Health Information Exchanges as Business Associates

- Business Associates now specifically include HIEs, RHIOs and PHR vendors.

Sale of EHRs or PHI

- Subject to certain exceptions, a Covered entity is prohibited from selling PHI unless the Covered Entity obtains the individual's authorization which includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the information.

Medical Record Requests

- If a Covered Entity has EHRs, the Covered Entity must provide an individual with a copy of his/her record in electronic format instead of hard copy and have it transmitted directly to a physician, hospital or another entity that they designate.
- The fee that a Covered Entity can charge for the transmission is limited to its "labor costs".

Marketing

- Currently under HIPAA, a Covered Entity may provide communications that might otherwise be considered marketing without individual authorization if the communication was to describe a healthcare operation, which includes an item or service or third-party payment for the item or service, for treatment, or for case management or counseling about alternative treatments.
- Under the HITECH Act, such communications are not healthcare operations, if the Covered Entity or Business Associate making the communication receives direct or indirect remuneration for making the communication. Direct or indirect remuneration will be defined consistent with federal fraud and abuse laws; however, payment for treatment is excluded from the definition of remuneration.
- Moreover, the change does not apply if:
 - The communication is about a current drug or biological that the recipient is taking, under certain circumstances, if the remuneration is "reasonable" (to be defined).
 - The communication is made by the Covered Entity based on a valid HIPAA authorization.
 - The communication is made by a Business Associate in accordance with a written business associate agreement.

Fundraising

- Individuals must be given a right to opt-out of receiving further fundraising communications. If an individual opts out, he/she will be treated as having revoked an authorization.

Enforcement

- DHHS will formally investigate any complaint of a HIPAA violation if a preliminary investigation of the facts of the complaint indicates a possible violation due to willful neglect.

Electronic Medical Records

- The Office of the National Coordinator for Health Information Technology (“ONCHIT”), which is a subdivision of DHHS, will expand the federal role in promoting and implementing health information technology high, creating profile roles for stakeholders, establishing a federal advisory committees and a stakeholders’ panel, and developing a new structure and process for developing and implementing HIT standards and specifications.
- ONCHIT will receive approximately \$2 billion for discretionary spending, primarily for grants and loans, and sets a goal that each person in the United States will have an EMR by 2014.
- Beginning in 2011, Medicare and Medicaid will provide financial incentives over multiple years of up to \$40,000 to \$65,000 per eligible physician and up to \$11 million per hospital for “meaningful” use of health information technology, such as electronic exchange of data and reporting of clinical quality measures.
- Starting in 2015, physicians and hospitals that do not use certified products in a meaningful way will be penalized.

Emily Kretchmer and William Mandell represent health care providers with compliance and health information matters.