



On February 17th, President Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA). A portion of the bill created the Health Information Technology for Economic and Clinical Health Act or the HITECH Act. The following summary covers areas of potential impact, key items to monitor and a section by section summary of Title XIII, Subtitle D – Privacy.

Changes with Potential Impact for Minnesota:

The HITECH Act attempts to clarify and expand the HIPAA Privacy and Security Rules, the new requirements include changes that may have an impact on Minnesota covered entities and business associates:

- Application of the HIPAA privacy and security requirements directly to business associates (BA);
- Establishing mandatory federal health information breach notification requirements for HIPAA covered entities (CE) and their business associates;
- Creating new privacy requirements for HIPAA covered entities and their business associates, including new accounting requirements for electronic health records (EHR), restrictions on marketing and fundraising, and other developments; and
- Establishing new criminal and civil penalties for non-compliance and new enforcement responsibilities.

Key Items to Monitor:

- Interim breach reporting regulations
 - Health and Human Services (HHS) Secretary to issue within 180 days, effective date 30 days later
- Minimum necessary and limited data set
 - HHS Secretary issues guidance within 18 months, limited data set sunsets
- Accounting for disclosure
 - HHS Secretary to promulgate regulations within 6 months after Health information technology (HIT) accounting standards adoption
- Prohibition on sale of EHR or protected health information (PHI)
 - HHS Secretary develops regulations within 18 months, effective 6 months later
- Vendor obligations for personal health records (PHR)
 - Federal Trade Commission (FTC) to promulgate interim final regulations regarding breach notice obligations within 180 days, to take effect 30 days after publication

Possible Next Steps:

- Be prepared
 - Review the changes with your legal counsel and HIPAA privacy and security officers. While most of the new requirements are not effective immediately, it will take some time to determine where your policies and procedures and HIPAA training will need to be updated.
- Watch for new rules and guidance
 - Monitor the development of HHS regulations and guidance documents issued under the HITECH Act. Anticipated publication dates for these rules and guidance documents are noted above. Please see the Minnesota e-Health Initiative web site for information regarding the proposed rules and guidance at www.health.state.mn.us/e-health/hitech.html.
- Respond promptly to compliance issues
 - Respond immediately to any information about potential HIPAA violations within your organization. The new penalty provisions are enforceable immediately against covered entities—with new enforcement authority by State Attorneys General.

Summary of Subtitle D, Privacy and Security Provisions, Part 1:

- *Sec. 13400 (Definitions)* clarifies that an EHR is “created, gathered, managed, and consulted by authorized health care clinicians and staff” while a PHR is “managed, shared, and controlled by or primarily for the individual”.
 - Breach definition - includes all “unauthorized acquisition, access, use, or disclosure of” protected health information; very limited exceptions to this definition apply if an employee unintentionally accesses PHI and there is no further access or disclosure; inadvertent disclosures, on the other hand, fall within the definition of a breach, unless the disclosure is made to another employee in the same facility.
 - Unsecured data – is defined as protected health information that is not secured through the use of a technology or methodology specified by the Secretary in the guidance issued under paragraph (2).
- *Sec. 13401 (Application of security provisions)* BA’s of CEs will now be directly subject to provisions of the Security Rule in the same way that CEs are, and that recognition of the administrative, technical and physical safeguards, and other applicable security procedures, must be incorporated in the BA agreement between the BA and the CE.
- *Sec. 13402 (Breach notification)* CEs must notify individuals and BAs must notify CEs upon the breach of unsecured data; regarding breaches, no ‘harm’ standard is included – individuals must be notified of any unauthorized acquisition, use, disclosure, etc. of their information whether or not such breach could or has resulted in any harm to the individual; notice to the individual must be made without unreasonable delay and in no case later than 60 days.
 - Breach notice provided to the individual must include – the date of the breach, the date of the discovery by the CE, the steps the individual should take to protect themselves from potential harm, the steps the entity is taking, etc.
 - Safe harbor for “protected” data – for PHI that is encrypted or otherwise rendered unusable, unreadable, etc. to an ANSI standard.
 - Interim final regulations regarding breach reporting are to be issued by the HHS Secretary within 180 days, with an effective date 30 days later.
- *Sec 13404 (Application of privacy provisions)* privacy provisions apply directly to BA and stipulates that HIPAA privacy requirements must be included in the BA agreement; the law also applies the Privacy Rule’s civil and criminal penalty provisions directly to BAs.
- *Sec 13405 (a) (Requested restrictions)* a CE must restrict disclosure of PHI to a health plan for purposes of payment or health care operations (not treatment purposes) at the request of the patient, if the patient self-pays for a service.
- *Sec 13405 (b) (Limited data set, minimum necessary)* CE must use a limited data set to the extent practicable or, if necessary, the “minimum necessary” when making a use or disclosure; the HHS Secretary is to issue guidance on “minimum necessary” within 18 months. After the Secretary issues guidance on what constitutes “minimum necessary” the limited data set guideline will then sunset.
- *Sec 13405 (c) (Accounting for disclosure)* CEs must account for all non-oral disclosures of PHI related to treatment, payment and health care operations (TPO) for a period of three years, if the PHI is maintained in an EHR; if the EHR is in place as of January 2009, the effective date for this requirement is 2014; if the EHR is deployed after January 2009, the effective date is either January 2011 or the date when the EHR system is acquired. In providing an accounting to individuals who request such, CEs may describe disclosures to BAs or provide a list of all BAs, which then must provide an accounting of disclosures on request. The HHS Secretary is to promulgate regulations on what information is to be included in the accounting within 6 months of adopting health information technology (HIT) technical standards on accounting; the regulations must take into account the interests of individuals and the administrative burden on CEs and BAs.

- Sec. 13405 (d) (Sale of EHRs or PHI) prohibits the sale of EHR or PHI obtained from EHRs absent an authorization by the individual; and neither a CE nor a BA can directly or indirectly receive remuneration in exchange for any PHI; with exceptions for public health activities and research, but any fees exchanged related to research would be limited to only the cost of preparation and transmittal of data. The HHS Secretary must develop regulations within 18 months, to be effective 6 months later.
- Sec. 13405 (e) (Individual right to electronic copy) a CE using an EHR must provide a copy of a patient's information in electronic format, with charges for providing such copies limited to the entity's labor costs. The individual may designate a third party, such as a PHR vendor, to receive this copy.
- Sec. 13406 (a) (Marketing) The new law prohibits a covered entity from obtaining direct or indirect payment for these types of communications: to describe a health-related product or service, for treatment of the individual, for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. An authorization must be obtained, except if the payment is for treatment or other limited circumstances. This provision applies in one year, on February 17, 2010, and applies to business associates.
- Sec. 13406 (b) (Fundraising) for non-profits, fundraising is now defined as a health care operation and individuals must be offered the choice of opting-out of fundraising communications.
- Sec. 13407 (Vendor PHR Obligations) Vendors of PHRs now have breach notification obligations, including notification of individuals and the FTC, similar to CEs and BAs. "Third party service providers" that provide services to PHR vendors must notify the PHR vendor if there is a breach of unsecured PHR and the FTC must notify the HHS Secretary of breaches it is notified of; there is safe harbor provisions for encrypted information. The FTC is to promulgate interim final regulations regarding these breach notice obligations within 180 days, to take effect 30 days after publication.
- Sec. 13408 (BA requirements for PHRs) requires BA agreements between CEs and Health Information Exchanges (HIEs), Regional Health Information Organizations (RHIOs) and any vendor that contracts with a CE to offer a PHR to patients as part of the CE's EHR.
- Sec. 13409 (Criminal Penalties) clarifies that HIPAA criminal penalties apply not only to CEs but to individual employees of CEs and other individuals.
- Sec. 13410 (Improved HIPAA Enforcement) strengthens HIPAA enforcement; increases the amount of civil monetary penalties under the HIPAA rules, and clarifies that State Attorneys General can bring lawsuits to enforce HIPAA.
- Sec. 13411 (Audits) The HHS Secretary shall provide for periodic audits of CEs and BAs that are subject to the requirements in Part 1.

Summary of Subtitle D, Privacy and Security Provisions, Part 2:

- Sec. 13424 (a) (Studies, Reports, Guidance)
 - Report on Compliance – an annual report from the Secretary of HHS to committees of the House of Representatives concerning complaints of alleged violations of the provisions under the HITECH Act and HIPAA. The report will include:
 - o Number of complaints
 - o Number of complaints resolved informally
 - o Number of complaints that resulted in civil or monetary penalties
 - o Number of compliance reviews and the outcome
 - o Number of subpoenas or inquires issued
 - o HHS Secretary's compliance improvement and enforcement plan
 - o Number of audits performed and summary of findings
- Sec. 13424 (b) (Studies, Reports, Guidance)
 - Study and report on the application of Privacy and Security for Non-HIPAA CEs – A study and report completed no later than one year after enactment of the HITECH Act. The study will specifically examine:
 - o Vendors of PHRs

- Entities that sell products on a PHR vendor website
- Entities that are not CEs but offer products and services on websites run by CEs that offer a PHR
- Entities that are not CEs that have access to, record, or send information to a PHR
- Third party service providers who assist in providing PHR products or services
- The report must be submitted to committees in the U.S. House of Representatives.
- Sec. 13424 (c) (Studies, Reports, Guidance)
 - Guidance on Implementation Specification to De-Identify Protected Health Information – Guidance completed no later than 12 months from enactment of this section. The guidance will focus on:
 - How to best implement the requirements for the de-identification of PHI
- Sec. 13424 (d) (Studies, Reports, Guidance)
 - Government Accountability Office (GAO) Report on Treatment Disclosures – A report completed no later than one year after enactment of this section. The report will focus on, best practices related to the disclosure among health care providers of PHI for purposes of treatment.
- Sec. 13424 (e) (Studies, Reports, Guidance)
 - GAO report required no later than five years after enactment of this section – A report on the impact of the privacy provisions included in the HITECH Act.
- Sec. 13424 (f) (Studies, Reports, Guidance)
 - Study by the Secretary of HHS – A study on the definition of “psychotherapy notes” with respect to inclusion of test data and materials used for evaluative purposes. The study has no specific timeline for completion.