



Recovery Act Significantly Changes HIPAA Laws

By Jeffrey J. Miller

April 2, 2009

The American Recovery and Reinvestment Act of 2009 significantly expands the HIPAA Privacy Rule and Security Standards through the addition of the Health Information Technology for Economic and Clinical Health Act (HITECH). The following is a summary of the key provisions of HITECH related to HIPAA.

A. Business Associates

HITECH applies HIPAA Security Standards, including subsequent penalties, to business associates directly and their covered entities. Under HITECH, covered entities and business associates must update their contracts to document this change;

- comply with the restrictions on use and disclosure of protected health information (PHI) of the Privacy Rule; and
- terminate the business associate agreement with a covered entity if the covered entity breaches its HIPAA obligations, and report the violation to the Department of Health and Human Services if it is not cured.

Failure to comply can result in civil and criminal penalties enforced by the Department of Health and Human Services.

B. Notification of Individuals of Breaches

Under HITECH, if unsecured PHI is breached, a covered entity must notify the individuals whose information was disclosed. It must provide notice of the breach to the Department of Health and Human Services and to prominent media outlets serving the applicable geographic area if more than 500 individuals were impacted.

C. Individual Access Right, Right to Request Restriction, and Accounting of Disclosures

HITECH expands an individual's right to access his or her medical record to include the right to receive an electronic copy of it, if it is available. HITECH modifies HIPAA by

- allowing covered entities to only charge individuals for the labor costs associated with providing the electronic copy;
- requiring that a health care provider honor a patient's request that their PHI not be disclosed to a health plan, if the patient paid out-of-pocket in full for that item or service;
- requiring a covered entity to give an individual the right to receive an accounting of PHI disclosures for treatment, payment, and health care operations during the previous three years, if the disclosures were through an electronic health record.



Recovery Act Significantly Changes HIPAA Laws

Effectively, these new rules require upgrading EMR software to track disclosures. Unfortunately, the law provides time for upgrades, but not for newly acquired systems. Therefore, the market will need to catch up to the legal requirements, which may slow implementation.

D. Minimum Necessary Standard

HITECH requires that covered entities limit the use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purpose. This requirement sunsets when the Department of Health and Human Services issues guidance on what constitutes minimum necessary. The Department of Health and Human Services has eighteen months to issue such guidance. Additionally, HITECH clarifies that the entity disclosing the PHI (as opposed to the requester) makes the minimum necessary determination. The HIPAA Privacy Rule's exceptions to the minimum necessary standard continue to apply.

E. Payment for PHI/Research and Public Health Activities

HITECH allows the sale of PHI by a covered entity or business associate without patient authorization in specified circumstances, such as

- to recoup the costs of preparing and transmitting data for public health or research activities; or
- to provide an individual with a copy of his or her PHI.

Within the next eighteen months, the Department of Health and Human Services is required to issue regulations governing the sale of PHI and the price covered entities may charge for the preparation and transmittal of the data. These provisions go into effect six months after the date of the final regulations. Note that the exceptions are limited and a covered entity may not receive remuneration from a third party for disclosures of PHI in connection with a health care operation such as case management and care coordination, or contacting individuals about alternative treatment options.

HITECH changes HIPAA's rules for marketing communications. Under HITECH, a communication by a covered entity or business associate that encourages patients to purchase or use a product or service is considered marketing, if the covered entity receives any form of payment in exchange for making the communication. Exceptions include

- communications describing a currently prescribed drug or biologic;
- payments received in exchange for the communication;
- a HIPAA authorization obtained from the recipient.

Under HITECH, the only exception to the prohibition are communications describing a drug or biologic currently being prescribed to the recipient and the payment to the covered entity is reasonable in amount. The meaning of "reasonable" is to be determined by the Department of Health and Human Services by regulation.



Recovery Act Significantly Changes HIPAA Laws

Presumably, refill reminders or educational materials about a drug currently being prescribed are acceptable, but switch letters are not acceptable (because they are not about the drug currently prescribed). Additionally, HITECH restricts educational communications to a specific patient population regarding a particular medication or treatment if the patients take that medication. This section goes into effect 12 months after enactment of the HITECH Act.

G. Enforcement and Penalties

In July 2005, the Justice Department addressed which persons may be prosecuted under HIPAA and concluded that only a covered entity (and not individual employees of the covered entity or unrelated third parties) could be criminally liable. HITECH provides that criminal penalties may apply to individuals, whether they are employees of the covered entity or otherwise. HITECH amends HIPAA by

- permitting the Office of Civil Rights to pursue civil monetary penalties against any individual for an alleged criminal violation of the Privacy and Security Rule of HIPAA if the Justice Department had not prosecuted the individual;
- requiring a formal investigation of complaints and the imposition of civil monetary penalties for violations due to willful neglect; and
- requiring the transfer of civil monetary penalties to the Office of Civil Rights to use in enforcing HIPAA.

HITECH increase penalties for violations of HIPAA by

- preserving the current requirement that a civil fine not be imposed if the violation was due to reasonable cause and was not corrected within 30 days; and
- authorizing state attorneys general to bring a civil action in Federal district court against individuals who violate the HIPAA privacy and security standards, in order to enjoin further violation and seek damages of up to \$100 per violation, capped at \$25,000 for all violations of an identical requirement or prohibition in any calendar year.

State action against a person is not permitted if a federal civil action against that same individual is pending. Nothing prevents the Office of Civil Rights from continuing to use corrective action without a penalty in cases where the person did not know, and by exercising reasonable diligence would not have known, about the violation.

HITECH requires the Secretary to perform periodic audits to ensure compliance with the Privacy Rule and Security Standards.

H. Effective Date

Except as otherwise specifically provided in the Act, these changes become effective 12 months after the enactment of HITECH.