Reinhart

Enhanced Federal Privacy and Security Protections for Health Information Underscore Need for Robust Privacy and Security Compliance Plan

POSTED:

Jun 1, 2009

RELATED PRACTICES:

Health Care

https://www.reinhartlaw.com/practices/health-care

RELATED PEOPLE:

Heather L. Fields

https://www.reinhartlaw.com/people/heather-fields

HIPAA Redux: The HITECH Act

Buried within Title XIII of the American Recovery and Reinvestment Act of 2009, which was signed into law on February 17, 2009, is the Health Information Technology for Economic and Clinical Health (HITECH) Act. In addition to allocating billions for development and implementation of health information technology, the HITECH Act contains far-reaching changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security regulations. Many of these changes will require the U.S. Department for Health and Human Services (HHS) to issue new regulations or guidance during the next two to 18 months to fully implement the new requirements.

Among the changes to the HIPAA privacy and security rules are the following:

New Accounting Requirements for Disclosures for Treatment, Payment and Health Care Operations

The HITECH Act adds a new patient right related to accounting of disclosures. Under the new provision, covered entities are required, upon a patient's request, to provide an accounting of all disclosures of protected health information (PHI) made through an electronic health record for purposes of treatment, payment or health care operations during the three years prior to the request. Unless delayed by the Secretary of HHS, this accounting requirement will begin to apply on January 1, 2014 to disclosures from an electronic health record acquired before January 1, 2009, and on January 1, 2011 to disclosures from an electronic health record acquired after January 1, 2009.

New Breach Notification Provisions

The HITECH Act adds new requirements for covered entities to notify patients whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed as a result of a security breach. The term "breach" is defined in the HITECH Act to mean unauthorized acquisition, access, use or

disclosure of PHI which compromises the security, privacy or integrity of PHI. The term does not include unintentional disclosures if made in good faith and within the course and scope of employment or a business associate relationship, and the PHI is not further acquired, accessed, used or disclosed. Required notification methods vary based on the number of individuals whose PHI has been breached.

Information that is "secure" is exempt from the breach notification requirement. In guidance issued on April 17, 2009, HHS stated that to "secure" information, a covered entity would need to protect the information by making it "unusable, unreadable, or indecipherable to unauthorized individuals." Essentially, this means that only encrypted health information would be deemed "secure."

Enhanced Penalties for Noncompliance and Enhanced Authority for Enforcement

The HITECH Act requires HHS to conduct formal investigations of complaints where a preliminary inquiry of the incident shows that "willful neglect" is the cause. In addition the new law increases the dollar amounts of civil penalties. Currently, the Office for Civil Rights (OCR) may impose a fine of $100 per violation with a cap of $25,000 for "identical violations per calendar year," however, a covered entity could raise an affirmative defense that it lacked knowledge or reasonable cause to know of the violation and avoid any penalty. The new law makes all violations subject to fines and creates a tiered penalty system with ranges for each tier. Fines for each single violation range from $100 up to $50,000 and the annual maximum penalty (the cap on annual penalties) ranges from $50,000 up to $1.25 million. HIPAA's criminal penalties will now apply to employees of covered entities and business associates. Finally, State Attorneys General will now be empowered to sue for actual or threatened HIPAA violations on behalf of residents of their state and obtain injunctions, statutory damages and attorneys fees.

The HITECH Act also creates new incentives for OCR enforcement efforts: civil penalties collected for privacy or security violations will be turned over to the agency to fund enforcement efforts. Many believe that this will cause OCR to shift its historically complaint-driven, compliance-oriented approach to enforcement to a more aggressive and punitive strategy.

Expanded Privacy and Security Obligations for Business Associates

The HITECH Act adds new responsibilities for business associates of covered entities, including making them subject to enforcement provisions and civil and

criminal penalties for HIPAA violations. Under the new provisions, business associates will be required to comply with many of the HIPAA security rule requirements previously only applicable to covered entities including the provisions related to the implementation of administrative safeguards (*e.g.*, implementation of policies and procedures to prevent, detect, contain and correct security violations; conducting (and documentation of) risk analysis and risk management); physical safeguards (*e.g.*, implementation of policies and procedures to limit physical access to electronic information systems and related facilities); technical safeguards (*e.g.*, implementation of policies and procedures creating unique user identification and tracking, authentication processes and transmission security, which may include encryption); and general requirements for policies and procedures and documentation of security efforts.

Next Steps

Stay tuned! Additional guidance and new regulations are expected to be issued later this summer. Over the coming months, covered entities should begin identifying policies and procedures, forms and agreements that will need to updated. In addition, in light of the expected increase in enforcement efforts, higher penalties for noncompliance, and new breach notification requirements, covered entities should review their existing security risk assessment and technical infrastructure and create a work plan to address any weaknesses. The general effective date for the general HITECH Act HIPAA provisions is February 17, 2010.