Reinhart

New Privacy and Security Requirements Under HITECH — Overview

This is the first in our series of Reinhart e-alerts about the Health Information Technology for Economic and Clinical Health Act (HITECH.) This e-alert provides an overview of HITECH as a refresher of our initial report in the Reinhart Employee Benefits Update for March 2009. We are also issuing a second alert today regarding the breach notification rules that were published on August 24, 2009. The Department of Health and Human Services (HHS) is expected to issue additional regulations interpreting the other obligations under HITECH, which we will address in future e-alert.

HITECH was signed into law on February 17, 2009. HITECH modifies and expands the privacy and security requirements applicable to covered entities (including multiemployer health plans) under the Health Insurance Portability and Accountability Act (HIPAA). This will require group health plans to take action to implement the new requirements.

HITECH makes significant revisions to HIPAA Privacy and Security Rules. New requirements under HITECH include the following:

- Business Associates. HITECH generally requires business associates to comply with HIPAA Privacy and Security Rules in the same manner as other covered entities (*e.g.*, health plans). Business associates will now have increased responsibility in safeguarding Protected Health Information (PHI) and disclosing instances where PHI has been accessed or shared. This change will require modifications to existing business associate agreements. This change becomes effective February 17, 2010.
- Breach Notification Rules. HITECH includes additional rules addressing the remedial steps a health plan must take if unsecured PHI is improperly disclosed or otherwise breached. These rules include additional notice requirements that were not included in the original HIPAA Privacy and Security Rules. The final regulations on these rules became effective September 23, 2009 and are discussed in a separate e-alert.
- Accounting for Disclosures. Under HIPAA, an individual has a right to receive an accounting of certain disclosures of his or her PHI by the health plan and business associates. HITECH requires health plans that maintain "electronic health records" to log routine disclosures for treatment, payment and health

POSTED:

Sep 28, 2009

RELATED PRACTICES:

Employee Benefits
https://www.reinhartlaw.com/practices/employee-benefits

RELATED PEOPLE:

Denise P. Goergen
https://www.reinhartlaw.com/people/denise-goergen

care operations. This is a significant change because under current law there is an exception which excludes disclosures due to treatment, payment and health care operations from the accounting requirements. Accounting for such disclosures is limited to three years (accounting for other disclosures remains six years). For electronic health records held by a health plan as of January 1, 2009, this requirement is effective for disclosures made on or after January 1, 2014. For records acquired after January 1, 2009, the requirement applies to disclosures on or after January 1, 2011. The HHS will be providing regulations on what information must be included in the accounting.

- Access to Electronic PHI. Under HITECH, a health plan that maintains "electronic health records" must allow individuals to receive an electronic copy of their own PHI upon request. A health plan must comply with an individual's request to transmit a copy of his or her electronic health record directly to an entity or person designated by the individual and may charge only labor costs. The provision becomes effective February 17, 2010.
- Marketing. In general, a health plan must obtain an individual's authorization to use PHI for "marketing" purposes. There are several exceptions to this requirement, including an exception for most communications that fall within the definition of "health care operations." If a health plan receives a direct or indirect payment by an outside entity to send a marketing communication to an individual, the communication will generally require prior authorization even if it falls under health care operations. The provision becomes effective on February 17, 2010.
- Restricting Disclosures. HITECH requires covered entities to agree to an individual's request not to disclose the individual's PHI for payment and health care operations where services for treatment have been paid in full out-of-pocket by the individual. This provision becomes effective February 17, 2010.
- Increased Penalties. HITECH significantly increases the civil monetary penalties for a violation of the HIPAA Privacy or Security Rule, effective this year.
- Limited Data Set/Minimum Necessary. Effective February 17, 2010, HITECH requires health plans to first limit the use, disclosure or request for PHI to the "limited data set" if practicable or, if needed, to the minimum necessary information to accomplish the intended purpose of the use, disclosure or request. HHS will be issuing new guidance on the "minimum necessary" standard for purposes of this requirement. A group health plan may continue to determine the meaning of the minimum necessary standard until HHS guidance is published.
- Sale of PHI. HITECH imposes new restrictions on the sale of electronic health records and PHI (*e.g.*, health plans cannot directly or indirectly receive

remuneration in exchange for any PHI unless the health plan obtains an authorization from the individual subject to certain restrictions). The effective date of this provision is six months after the date HHS issues final regulations. HHS guidance is expected no later than August 17, 2010.

The HITECH requirements are generally effective February 17, 2010, although certain provisions contain different effective dates (as noted above).

NEXT STEPS. Health plans should take the following steps to comply with HITECH's new requirements:

- Review and update business associate agreements.
- Determine whether any activities would be considered "marketing," and how to comply with new limitations on such activities.
- Review and update electronic PHI accounting procedures and forms.
- Update HIPAA Privacy Notices, as necessary.
- Revise HIPAA Privacy and Security plan amendments, as necessary, to reflect the new requirements.
- Update HIPAA policies and procedures, as necessary, to reflect the new requirements, such as processing individual requests for electronic health records and requests to restrict PHI disclosure.
- Determine when it may be practicable to disclose PHI in a limited data set.