Reinhart

New Privacy and Security Requirements Under HITECH — Final Regulations on Breach Notification

This is the second in our series on the new Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security requirements imposed by the Health Information Technology for Economic and Clinical Health Act (HITECH).

On August 24, 2009, the Department of Health and Human Services (HHS) published interim final regulations on the new breach notification rules under HITECH. Under HITECH, a covered entity (which includes a group health plan) with "unsecured" Protected Health Information (PHI) must notify each affected individual in the event of a breach. Key points in the final regulations include the following:

- **Securing PHI**. The HITECH breach notification rules apply to "unsecured" PHI. In April 2009, HHS issued a safe harbor rule that indicated encryption and destruction are the only two ways to secure PHI. The final regulations clarify that this guidance does not impose a new requirement that health plans encrypt all PHI. For purposes of the HIPAA Security Rule, a health plan may rely on firewalls and other access controls instead of encryption. However, such PHI would be considered "unsecured" for purposes of the breach notification rule.

- **"Risk of Harm" Test**. A breach occurs if PHI is used or disclosed in a manner not permitted by HIPAA and such use or disclosure "compromises" the security or privacy of the PHI. Notice is required only if a breach occurs. In reviewing whether PHI was compromised, a health plan would analyze various factors including the nature of PHI disclosed, the recipient of the PHI and whether the unauthorized use or disclosure poses a significant risk of financial, reputational or other harm to the individual. Health plans will need to perform risk assessments to determine whether notification is required. Health plans should retain sufficient documentation to demonstrate that a thorough risk assessment was conducted to determine whether or not a breach occurred.

- **Breach Notification Requirements**. The final regulations set forth the requirements for breach notifications including specifications for content, methods of delivery and timing. Notification must generally be made within 60 days of discovery of the breach and must satisfy certain content requirements (e.g., describe the date and circumstances of the breach and the type of PHI involved). Additional requirements apply for breaches that involve more than

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

500 individuals in a state or jurisdiction. HHS must receive notice if a breach involves 500 or more individuals. For breaches involving less than 500 individuals, the group health plan must maintain a log of breaches and annually submit it to HHS.

The final regulations are effective September 23, 2009. However, HHS indicated that due to the short compliance deadline it will not impose sanctions for failure to provide the required notification for breaches that are discovered before February 22, 2010 — although health plans are expected to comply with the requirements.

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

- Analyze the extent to which PHI can be encrypted or destroyed to meet HHS's safe harbor for securing PHI. Again, this is not required, and may be difficult, but it can be beneficial because the plan would no longer be subject to the new breach notification rules (but would, of course, still be subject to other general privacy and security obligations under HIPAA).
- Develop procedures for identifying and responding to breaches of unsecured PHI (including risk of harm assessments) and for keeping a log of breaches for annual reporting to the HHS.
- Prepare a model breach notification letter.
- Train employees on the new breach notification requirements, disposal of PHI and other new requirements.