Reinhart

HIPAA Developments Signal Need to Assess Current Security Rule Compliance for Hospice and Long Term Care

Recent enforcement actions by the Department of Health and Human Services (HHS), Office of Civil Rights (OCR) underscore a continued focus on compliance with the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations, particularly the Security Rule. Deficiencies in covered entity HIPAA Security Rule compliance has been documented by prior OCR audits and has caused many of the reported large-scale breaches. Although many smaller health care providers and their business associates cite the lack of internal information technology expertise and resources as significant obstacles to HIPAA Security compliance, OCR's enforcement record demonstrates that these factors will not shield even smaller sized organizations from significant fines for Security Rule noncompliance. In addition to assessing mobile device security, covered entities and their business associates would be well-served to review OCR's HIPAA Security Rule compliance resources, including the new risk assessment tool published in the spring of 2014.

POSTED:

Aug 5, 2014

RELATED PRACTICES:

Health Care

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

RELATED SERVICES:

Hospice and Palliative Care

https://www.reinhartlaw.com/services/hospice-and-palliative-care

OCR HIPAA Enforcement Continues to Focus on Mobile Device Security and Encryption

In December 2013, OCR settled an investigation against a small Massachusetts dermatology practice following the loss of a thumb drive containing electronic protected health information (e-PHI). Like many OCR investigations, it began after an individual reported the incident to OCR. The investigation revealed that the dermatology practice failed to conduct an accurate and thorough analysis of the potential risks to and vulnerabilities of the confidentiality of electronic e-PHI, and further, that the dermatology practice failed to fully comply with the Breach Notification Rule by not having written breach policies and procedures. Notably, this case marked the first settlement against an entity for not having such policies and procedures in place. The settlement included $150,000 in fines and a corrective action plan requiring the development of a risk analysis and risk management plan. Commenting on the settlement, then-current OCR Director Leon Rodriguez stated that "covered entities of all sizes need to give priority to securing electronic protected health information."

Reinhart

Similarly, in January 2013, OCR settled an investigation against a small Idaho hospice following the loss of an unencrypted laptop computer containing the e-PHI of approximately 400 patients. Over the course of its investigation, OCR discovered the hospice had not conducted a risk assessment to safeguard e-PHI, nor did it have written policies and procedures addressing mobile device security, as required by the HIPAA Security Rule. The settlement included a $50,000 assessment. This case marked the first settlement of its kind for a breach involving fewer than 500 patients.

Recent settlement agreements also reveal OCR's focus on encryption efforts. In April 2014, OCR settled investigations of the theft of unencrypted laptops from two entities: a Missouri physical therapy center and an Arkansas health plan. The settlements involved fines of $1,725,220 and $250,000, respectively. OCR's investigation found that although the Missouri physical therapy center had identified the risk of using unencrypted laptops and was indeed taking steps to begin encryption at the time of the laptop's theft, the entity's efforts "were incomplete and inconsistent over time." The Arkansas health plan was found to have failed to comply with multiple requirements of the Privacy and Security Rules, including failing to implement policies and procedures to prevent, detect, contain and correct security violations.

OCR's HIPAA Risk Assessment Tool Marketed at Small- and Medium-Sized Providers

In an effort to improve Security Rule compliance, OCR and the HHS Office of the National Coordinator for Health Information Technology developed an assessment tool to help smaller health care providers conduct and document their risk assessment in a methodical and organized manner. Although the assessment tool does produce a report the provider may submit to auditors, it does not automatically send out data after it is entered. The assessment tool is available for download on HealthIt.gov, along with a user guide and tutorial video.

Action Steps

Health care entities and their business associates should evaluate the current status of their HIPAA Security Rule compliance efforts. Among the actions that may be considered are the following:

- **Review Current and/or Conduct a Security Risk Assessments**: A risk

assessment is intended to be a "living" document that is updated and reviewed at least annually. In addition to annual reviews, the risk assessment should be updated whenever the entity experiences a change that could pose new security or privacy issues, such as the adoption of new information technology systems or software updates. If an entity has not already done so, it should conduct thorough risk assessments of its operations. Risk assessments should address any unique aspects of the operation, including mobile device security and data encryption risks. Smaller entities should consider using the new HHS risk assessment tool to work through the process.

- **Implement a Risk Management Plan**: Following the initial risk assessment, an entity should develop and implement a risk management plan aimed at reducing any identified risks and vulnerabilities to a reasonable level. Further, the risk management plan should be updated following any updates to the risk assessments.
- **Update Policies and Procedures and Train Staff**: As the recent enforcement actions demonstrate, it is important for entities to have written policies and procedures addressing, among other things, breach notification and mobile device security. Additionally, staff members should receive adequate training so that they understand and can effectively implement the policies and procedures.

In summary, regardless of size or complexity of operations, it is as important as ever for providers and their business associates to take proactive steps to ensure the effectiveness of their HIPAA compliance efforts. The Health Care team at Reinhart Boerner Van Deuren s.c. is available to assist you in developing and implementing a HIPAA compliance plan, including developing a risk assessment and risk management plan, or to consult with you regarding developing written policies to address breach notification or mobile device security, or any other legal or regulatory issues.

Please feel free to contact a member of Reinhart's Health Care team or your Reinhart attorney to discuss any questions or concerns related to your health care entity.