Health Information Compliance Alert

Keep Your Conscience Clean with Better Risk Management

Tip: Scrutinize your analysis, then put a course of action in place.

The issues that tripped up University of Texas MD Anderson Cancer Center (MD Anderson) are easily avoidable. Organizations must use the information gleaned from their risk assessments to fully implement and manage a working HIPAA system, especially with more and more encryption issues like this coming down the pike.

"The recent ruling by an Administrative Law Judge (ALJ) against MD Anderson provides insight into several areas of HIPAA compliance and the government's enforcement thereof," explains attorney **John E. Morrone, Esq.**, a partner at **Frier Levitt Attorneys at Law** in New York.

Review Morrone's eight takeaways from the ALJ decision:

- MD Anderson recognizes the vulnerability of non-encrypted portable electronic devices and drafted policies to address the risk but did not follow their own policies.
- Loss or theft of portable electronic devices are one of the most significant causes of breaches of PHI.
- The loss of portable devices can affect a staggering number of individuals. Here, over 33,000 patients were affected.
- The ALJ demonstrated substantial deference to the agency [and] is upholding the $4.3 million fine.
- [HHS Office for Civil Rights] OCR demonstrated how aggressively it will pursue non-compliance by covered entities [CEs].
- Covered entities need to have robust compliance plans, which they implement and follow.
- Data encryption is an essential element in protecting ePHI and avoiding expensive penalties.
- Merely losing an unencrypted device constitutes a data breach under HIPAA, so encryption is truly the best method to avoid a HIPAA breach.

Reminder: An assessment reviews how a breach would "negatively impact" your ePHI, suggests the OCR in its Q-and-A on the difference between risk analysis and risk management. When you analyze, you "consider all relevant losses that would be expected if the security measures were not in place," the agency guidance notes. Management of that risk involves the way your practice implements HIPAA controls from the gathered data and emerging threats.

Read the OCR Q-and-A at www.hhs.gov/hipaa/for-professionals/faq/2013/what-is-the-difference-between-risk-analysis-and risk-management-in-the-security-rule/index.html.

CPT® 2023 American Medical Association. All rights reserved.