Health Information Compliance Alert

Reader Question: How Much Will The 2016 OCR Audits Focus On Risk Management?

Question: We're hearing that the 2016 HIPAA audits will focus a lot on risk assessments. Is this true?

Answer: Although the 2016 **HHS Office for Civil Rights** (OCR) audit protocol covers more of the HIPAA regulations than the prior protocols, risk management is certainly a big focus.

In the 2012 audit protocol, OCR didn't even have an audit inquiry for risk management but the 2016 protocol now does, according to an April 11 blog posting by **Bob Chaput**, CEO and founder of **Clearwater Compliance LLC**. "Not only will the auditors be looking for policies and procedures for a risk management process, but also the details of how risk will be managed, by whom, how often, and documentation of management's acceptable level of risk."

Auditors will also want evidence that you've implemented security measures as a result of your risk analysis, and that those measures are sufficient to mitigate or remediate identified risks to an acceptable level according to the risk rating, Chaput said.

Another new audit inquiry for 2016 is assessing "criticality" of specific applications and data with respect to other components of your contingency plan, Chaput stated. Auditors will specifically review your policies and procedures for assessing application and data criticality, and then review the list of critical electronic protected health information (ePHI) applications and the criticality levels you assigned to them.

The protocol provides that the auditors must ensure that the assigned criticality levels "should have been categorized based on importance to business needs or patient care, in order to prioritize for data backup, disaster recovery, and emergency operations plans."

Beware: Overall, the audit processes related to risk management "have become significantly more comprehensive," Chaput warned. "Now, in addition to looking for the who, what and how in the policies and procedures, audits will be requesting evidence of management's involvement in determining an acceptable level of risk, risk-rating registers, and a determination of the sufficiency of security measures put in place for mitigating or remediating identified risks."