Pain Management Coding Alert

Reader Question: Take Steps, Be Prepared if OCR Comes Calling

Question: In addition to being the coding lead at our practice, I'm also part of our risk management team. Another team member told me that Health Insurance Portability & Accountability Act (HIPAA) audits are going to focus on risk assessments in 2016. Is this true?

Nevada Subscriber

Answer: The Office for Civil Rights' (OCR) updated audit protocol will cover a lot more HIPAA regulations than any of the prior protocols. And yes, risk management is certainly a big focus for the Feds in 2016.

OCR a branch of the Department of Health and Human Services (DHHS) last updated the protocol in 2012. Back then, the plan didn't even have an audit inquiry for risk management. The 2016 protocol changes that, according to a blog post by **Bob Chaput**, CEO and founder of Clearwater Compliance LLC in Florida.

"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," explained Chaput.

Impact: 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."

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.

Also: 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."