Codify
BY AAPC

Health Information Compliance Alert

Reader Questions: Know the Facts on Hiring HIPAA Audit Help

Question: Our large, primary care practice takes HIPAA very seriously, and we do our best to maintain compliance with the rule. At our last planning meeting, we realized it's time to do another annual HIPAA risk assessment. Since it is a requirement under the HIPAA Security Rule, should we hire an outside consultant to do the assessment and analysis or is it ok for our compliance officer or IT manager to perform the audit?

South Carolina Subscriber

Answer: No, it is not legally necessary to engage an outside HIPAA expert to perform your annual risk analysis. But that being said, it's never a bad idea to have more than one opinion on ways your practice can decrease its chances of a violation.

The size, scope, and specialty of your organization usually determines the necessity of an outside resource. But, if the same person who does the assessment manages the implementations both monthly and annually, it might be a good idea for a change. "I think it is good to engage an outside consultant, to ensure that those issues that staff may be blind to can be revealed," advises **Jim Sheldon-Dean**, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, Vermont.

Sheldon-Dean adds, "But, reviews can also be internally directed, and it can be useful to have a mix, alternating reviews by internal or external parties, or alternating between two external parties."

An outsider can look at your practice challenges objectively and is more likely to call out issues that staff may purposely ignore, particularly as the majority of breaches are caused from insider threats.

"I doubt that insider issues would affect the risk analysis, since the risk analysis will dictate what needs to be done for security, but leave the investigation of what's gone wrong to the processes instituted according to the risk analysis," Sheldon-Dean cautions. "Doing the risk analysis, whether by internal or external parties, will result in exposing the need to look for improper insider activity, which is a required but often ignored process."