Codify
BY AAPC

Health Information Compliance Alert

HIPAA Audit: Pull Your Act Together With These Pointers

It's never too late to start getting into compliance.

Assemble a team: "Covered entities should be assembling a team to review all privacy and security policies, procedures and practices, and should update and revise them as needed," **Kenneth Rashbaum, Esq.** of Rashbaum Associates in New York tells **Eli**. The team should be comprised of IT, health information management (known as medical records in some institutions), in-house counsel, the chief information security officer and/or an outside technology consultant experienced in security analyses, outside counsel with experience in HIPAA privacy and security compliance, and representatives of clinical departments (end users)," he adds.

Rashbaum's suggestion for bringing in outside counsel stems from the realization that in-house counsel may find themselves in an awkward position if they attempt to advise the work force prior to and during the audit, as in some states the privilege protections for in-house counsel are not as strong as they are for outside counsel.

What Covered Entities Should Be Doing -- And Equally Importantly -- Not Doing

Risk assessment: "If the covered entity has not done so recently, it should immediately begin the process of conducting and documenting a HIPAA Security Risk Analysis, as required by the Security Rule," Rashbaum warns us. "The U.S. Department of Health and Human Services has issued a guideline on the requirements of this Risk Analysis. The team referenced above should facilitate it, with outside counsel receiving reports from the team members and preparing the documentation of the risk analysis."

Every bit of effort you can show helps avoid violations and penalties, points out **Jim Sheldon-Dean**, Director of Compliance Services, Lewis Creek Systems, LLC in Charlotte, Vt. There are some sources for questions that have been asked in prior audits which can be found at the links given below. "Those questions should be reviewed," he says. When you "feel comfortable answering those questions, you can start to feel comfortable about being audited." But it takes a real information security compliance effort to really be able to honestly feel comfortable with those questions, he adds.

Note: You can look for questions at these links:

- 42 questions asked in first OIG HIPAA Security audit in March 2007 at http://tinyurl.com/2ac9jm.
- CMS OESS 2008 Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews, at http://tinyurl.com/27eakjz
- Questions asked of a small provider after a data breach involving theft of a laptop and server, at: http://tinyurl.com/3jpoa4p

As a covered entity you should, during this period, avail your organization of all required safeguards and precautions with regard to uses, storage and disclosures of electronic health information, and should avoid activities that may lead to a breach, Rashbaum reminds us. You should enhance monitoring of compliance with safeguards and precautions for management of electronic health information, and document the steps taken to monitor compliance. "Particular attention should be paid to preservation of information relevant to security and privacy protocols; such documentation should be protected from loss or destruction," he advises.

What to avoid?

Documentation is critical: "Don't put off the work needed for a real HIPAA security risk analysis and mitigation effort," says Sheldon-Dean. If you do a good job now and document it properly, you will have an easier time staying compliant in the future and being ready for any audits. If you avoid the issue, you may be liable for willful neglect penalties that start

at $10,000 per day, he warns.

Be cooperative: The authorities want to help everyone be compliant, and they can help, not just find potential violations, Sheldon-Dean says. If they do find violations, they may want to initiate an enforcement action, but that's not a given. It's more likely that they'll find security deficiencies that are not violations of the rules themselves but could lead to violations, especially if there hasn't been an organized HIPAA security compliance effort before now, he says.

Remember: What auditors want to see is evidence of policies and procedures, and that the policies and procedures have been used to achieve their aims -- in short, documentation, Sheldon-Dean says. The more you can have a good information security process documented, the easier it is to respond to audits. All you have to do is point to the evidence of your work, and that makes life easier for everyone. Even if it's only initial documentation of planning for the process you just decided to start yesterday, it's still better than nothing, he says. Every bit of effort helps to show auditors that you take security seriously, which is the point.