Health Information Compliance Alert

SECURITY: Analyze This! Or Face Security Rule Risk

5 Easy Steps To Set Up Your Risk Analysis Plan

Even though you likely performed a risk analysis when you prepped for HIPAA's privacy rule compliance deadline, the security rule is a completely different regulatory animal. Here's some expert advice on how to beat the security rule beast.

ONE: DISTINGUISH BETWEEN RISK A**NALYSIS AND RISK ASSESSMENT - BUT DO BOTH.** A risk analysis is far different from the risk assessment you may have already performed as part of your HIPAA prep work. An assessment involves applying the HIPAA security rule provisions to identify vulnerabilities in your organization, while the risk analysis identifies threats -confidentiality or data integrity breaches, unauthorized access to systems, or improper fax transmissions, as well as physical threats like unlocked doors or cabinets, as just a few examples - that would exploit those vulnerabilities and clarifies the level of risk these security threats present, says **Margret Amatayakul** with **MargretA Consulting** in Schaumberg, IL. But remember, first thing's first. You must identify vulnerabili-ties before you can analyze threats.

TWO: MAKE ONE PERSON R**ESPONSIBLE, BUT PROVIDE LOTS OF HELP.** Your organization should assign responsibility for security rule compliance to one person - ideally for the position of security rule officer - but that officer should receive aid and input from a variety of people within your institution, advises Amatayakul. Don't limit your risk analysis to IT folks, she advises, "because IT professionals do not consider external or socio-political threats" to your organization.

She also notes that risk analysis is new to health care, and says whether you perform one in-house or you decide to use an outside facilitator, senior management has to be a part of the process.

THREE: SCALE YOUR THREAT L**EVEL: HIGH, MODERATE, AND LOW.** Once you've identified your organization's vulnerabilities, it's time to assign each threat a level of risk, from high to low. Your security officer, IT profession-als and others should be involved in this process. Once that's accomplished, you can begin to assess the probability that a security breach may occur, and that's one of the toughest parts of a risk analysis, says **Phil Banks**, an attorney in the Chicago office of **Deloitte & Touche**.

"There aren't too many crystal balls or fortune tellers to tell you what's the probability of a certain threat being realized at your hospital," laments Banks. However, "sooner or later, someone has to decide whether a threat is likely enough to occur and that it justifies the cost. Whoever you are, just don't do it alone," he advises.

Also, you'll want to assess your risk level in combination with the complexity, expense or degree of difficulty to mitigate that risk, says **Russell Opland**, Chief Privacy Officer/HIPAA Coordinator for the **University of Pennsylvania Health System** in Philadelphia. "You might come up with something that's a high priority but if it's also incredibly complex or expensive, then that's going to bump it down. You're probably going to look for something that has the biggest bang for the buck - lower complexity or lower cost but high risk would be things that you'd target first," he offers.

FOUR: DOCUMENT YOUR EFFORTS. Since there are so many people involved in risk analysis, it's a great idea to document how you analyzed threats and determined your organization's vulnerabilities. That's especially significant if a security breach occurs and the **HHS' Office for Civil Rights** wants to know why. Documenting the risk analysis process shows that you've been diligent, insists **Reed White** with the Chicago office of Deloitte & Touche. It reveals to anyone who wants to know that it was a formal process and you incorporated the advice and concerns of a whole team of individuals when you analyzed your threats. "[It shows] how you came up with your findings; it was a formal process and

it was logical, and it required some research, and so on," White tells **Eli**.

FIVE: GO LITTLE BY LITTLE, BUT START NOW. If preparing for the privacy rule compliance deadline taught you only one thing, it's that time flies when you must comply. Amatayakul says get started on you risk analysis program A.S.A.P. She says there are many people starting to say, "well, maybe we should do this now, because we know two years goes by pretty fast - we've learned that from privacy rule compliance." In addition to that, you may have bigger ticket items to buy with security rule compliance, and you'll need to find out what those are so you can budget for them. "[My clients] may not act upon stuff right away, [but they] realize that they do need a risk analysis fairly early on."