Health Information Compliance Alert

Reader Question: Know the Rules on Documenting Your Risks

Question: We are in the beginning stages of our annual risk assessment. Is there a format we should follow or contract we should download to make it official?

Michigan Subscriber

Answer: Though it might seem like the **HHS Office for Civil Rights** (OCR) has a template for everything, they do not have a set formula or outline for risk analysis documentation.

Here's why: Your risk analysis process may look entirely different from another provider's approach, but you'll probably have some similarities if you plan on including all of the HIPAA Security Rule requirements in your protocols. Plus, if you want to stay in the OCR's good graces, you'll need to thoroughly document your risks - and how you plan to manage them.

"It's very difficult to have a standardized, one-size-fits-all kind of approach," says HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at **Lewis Creek Systems LLC** in Charlotte, Vermont. "Every organization is different and has a different way of approaching [its] risk analysis."

You must have procedures for reporting, processing, and responding to suspected or known information security risks and incidents, Sheldon-Dean stresses. These procedures are essential for investigating, mitigating, and documenting your current risks and possible future security incidents, so that you can appropriately report and promptly handle violations and breaches - and the more comprehensive your finalized documentation, the better.

Reminder: Though a specific format isn't required, "the risk analysis documentation is a direct input to the risk management process," OCR cautions in its Security Rule summary.