

OASIS Alert

HIPAA: Is Your OASIS Data Safe?

It's not a good idea to turn a blind eye on HIPAA compliance.

Each OASIS assessment you complete includes personal health information about the patient. Increased scrutiny of your agency's HIPAA compliance is almost at hand. Make sure you're ready to weather the test.

You may have heard inklings of other providers undergoing HIPAA audits, but because the scope of the audits was so small, you didn't prepare for one yourself. That's all about to change, as the **HHS Office for Civil Rights'** pilot HIPAA audit program comes to a close, and the permanent audits begin in October.

You can prepare now for the audits that could be coming your way using a few simple tips that **Jim Sheldon-Dean**, director of compliance services at **Lewis Creek Systems**, shared during a recent **Coding Institute** audioconference, "The HIPAA Audit Protocol □ Documenting Compliance Before You Get an Audit Notice."

You Can't Wait Until 2014

If you heard that HIPAA audits don't begin until 2014, you're both correct and incorrect. "They say the new audit program is beginning in 2014," Sheldon-Dean says. "But of course what they're talking about is the federal fiscal year 2014, which begins on Oct. 1, 2013."

Keep in mind, however, that auditors aren't trying to fill a quota of nailing providers on broken privacy laws. "Enforcement is not the point of the audits," Sheldon-Dean says. "The point of the audits is to review compliance and find problems. But if they see a problem that may be worth some kind of enforcement action, they're not averse to discussing that with those who would be going in to levy the fines."

The penalty that you may not be familiar with, because it's new, is the penalty called "Willful Neglect," Sheldon-Dean says. "It means if you have not been paying attention, if you have not been doing what you should be doing for compliance and there's some kind of problem, they can levy some significant fines. It gets very expensive very quickly, so you want to make sure you don't ignore the rules."

Willful Neglect penalties are assessed only when you fail to implement HIPAA into your agency and continue to follow up on ensuring your compliance with HIPAA requirements. So, providers that have a HIPAA breach despite their best effort in maintaining privacy and security shouldn't be affected by the new penalty.

Consider Risk Assessment

To confirm that your organization is operating effectively under the HIPAA guidelines, you should perform a risk assessment, Sheldon-Dean suggests. You don't need to perform one more than every year unless you're installing new systems, hiring new business associates, or making any other significant changes that could alter your privacy and security compliance.

Although the government does not offer a risk assessment tool per se, the **National Institute of Standards and Technology** does publish risk assessment guidelines in its document "An Introductory Resource Guide for Implementing

the HIPAA Security Rule." The document guides you in how to identify realistic threats to protected health information (PHI) in your agency as well as potential vulnerabilities. You'll then weigh those against your current security controls to determine your actual risk level. You can access the document at

<http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>.