Health Information Compliance Alert

Reader Question: How Often Do You Really Need To Perform A Risk Assessment?

Question: We are having a bit of a debate in our practice. Some of us think that performing a risk assessment once every few years is adequate, but others believe that we should do them more often. How often should our practice perform a risk assessment?

Answer: The answer is not the same for every organization and every situation. You should generally "take a good scan around and make sure you've covered all your bases at least once every couple of years," says **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC,** based in Charlotte, VT.

If nothing much in your practice is changing and you're continuing to do business the way you always have been, performing a comprehensive risk assessment every couple of years is sufficient.

Caveat: But if you know you're making a change for example, if you're installing some new systems or changing how you're doing business you need to perform a risk assessment to pinpoint any risks and determine whether the change alters any of your risk profiles, Sheldon-Dean stresses.

Another exception to keep in mind is meaningful use funding, Sheldon-Dean points out. If you're getting federal money for your electronic health record (EHR) system, you'll need to update on an annual basis so you'll need to perform a risk assessment on a yearly basis as well.