As Seen In
HEALTHCARE MANAGEMENT + TECHNOLOGY TODAY

Why I Recommend a Security Risk Assessment to My Clients

Article by Stacey L. Gulick
Partner, Garfunkel Wild, P.C.

As someone who advises my clients regarding regulatory and cybersecurity matters, I have noticed a substantial increase in interest in data security. I work with healthcare providers of all types, from large hospitals to small practices and insurance companies, as well as the business associates that partner with them.

The bottom line is this: it is absolutely essential to have a security risk assessment (SRA). The SRA is required under the HIPAA Security Rule. As a result, the OCR will request a copy of the SRA whenever it has cause to initiate an investigation as a result of a complaint, breach or desk audit. I've been involved in a lot of OCR investigations and I can tell you without exception, if you are being investigated, the very first thing the OCR will ask to see is your SRA. **Every single time**.

The covered entities and business associates I work with usually ask how to come into compliance with HIPAA. Some think it's merely giving out the privacy notice, while others think they've purchased a "HIPAA-compliant" app or EHR. The reality is there is no software program to make your organization compliant. It's ongoing work monitoring and remediating as you create a culture of compliance.

The first step to establishing such compliance is to identify risks and vulnerabilities and implement a plan to address those issues. Without a comprehensive SRA that takes into consideration all of a facility's computer systems, software, and hardware, it is impossible to fully identify and prioritize each area of vulnerability. The SRA and associated plan also allows for an effective tool to communicate with your CFO, CEO, and IT team regarding the status of cybersecurity initiatives and empowers you to make intelligent decisions about budgeting.

It is important for you to remember that you cannot have an SRA conducted one time and think that your obligation is fulfilled. The standard under the Security Rule is that the SRA must be "up-to-date". Meaning, any time that there is a change in computer systems, location, or policy, the SRA must be updated. For many providers, updating the SRA annually ensures compliance.

A word of caution: internally-conducted SRAs are typically fraught with problems. Very few healthcare professionals are completely up-to-date with security, or the current HIPAA compliance guidelines. I advise my clients to have an external expert conduct the SRA in order to advise on vague or confusing aspects of HIPAA.

For example, I get a lot of questions about encryption. The reality is, HIPAA does not require encryption – it's an addressable standard. Nevertheless, the OCR will seldom accept explanations for the lack of encryption. As a result, there have been settlements with significant payments for failure to address this issue in the SRA on an ongoing basis.

In closing, let me add that thinking budget restrictions make an SRA unaffordable is flawed by design. Whether your organization is large or small, the OCR will levy higher fines for a lack of an SRA. And, dollars are only the first loss – loss of reputation can exceed fines in damages to your overall business.

About the Author: Ms. Gulick has extensive experience in health care administration, having worked as a medical staff coordinator, risk manager and compliance officer for several years prior to becoming an attorney. Her practice includes representation of healthcare providers and their business associates in implementation of HIPAA compliance programs, OCR investigations, HIPAA Breach responses, and various cyber security and interoperability issues.

To learn more about Security Risk Assessments, visit www.ClearDATA.com.