Health Information Compliance Alert

Vendors: Know the Ins and Outs of a Security Risk Analysis

Tip: It's more than just policies and procedures.

Your practice likely struggles daily to safeguard not only all your mobile and medical devices but also your patients' data. However, accidents do happen despite the best intentions, and top-notch HIPAA security compliance doesn't always go as planned.

After a devastating breach, one of the first things the **HHS Office for Civil Rights** (OCR) will ask for is your risk analysis and an outline of how you've managed and mitigated your security issues. Remember, your primary goals are to dually protect your patients' electronic protected health information (ePHI) and your practice data.

If you're in the market for a new IT vendor, you may want to discuss their understanding of the HIPAA Security Rule and all that entails.

Read on for expert advice on IT vendor vetting.

Check Locally First

It's always easier to hire IT help familiar with your specialty or who understand the geographic disposition of the area in which you practice. "Look for an IT vendor that works with other medical practices in the area," says **Adam Kehler**, principal consultant and healthcare practice lead with **Online Business Systems**.

You also want to find a vendor who knows the nuances of the software your organization utilizes. "It is especially helpful if they are knowledgeable in the EMR system the practice uses," Kehler advises.

Seek a Cybersecurity Expert Beyond the Bounds of Your EHR Vendor

When engaging a security expert, it's a good idea to look at firms other than your EHR or EMR provider. "I recommend using a cybersecurity firm that is separate from the IT vendor," stresses Kehler. "This is for a few reasons: IT vendors typically don't have the expertise to conduct a security risk analysis in accordance with the requirements of the HIPAA Security Rule."

He continues, "Second, you don't want your vendor assessing their own security since there is an inherent conflict of interest. Their motivation is to under-report security risks because it makes it seem like they aren't doing their job properly."

Choose a Vendor Familiar With the HIPAA Security Rule and Risk Analyses

It is critical that your cybersecurity team not only recognizes the nuances of the HIPAA Security Rule, but that they can expertly perform security risk assessments and analyses - plus manage the problems the audits uncover. "When evaluating a vendor for a security risk analysis, evaluate their process," Kehler says.

According to Kehler, a security risk analysis is not:

- A network scan
- A description of security controls
- A HIPAA gap analysis (i.e. description of how the organization meets the requirements)
- A vulnerability scan or penetration test.

That's why you must check your vendor's knowledge and ensure that they know the requirements. A proper security risk analysis should include the following, Kehler says:

- An inventory of ePHI throughout the organization
- A consideration of threats and vulnerabilities
- An evaluation of administrative, physical, and technical security controls
- A calculation of residual risk to ePHI

Resource: Review the HIPAA Security Rule at www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.