6 Things to Ask your EHR Vendor about Security

October 12, 2017 | EHR [1], Contracts [2], Health IT [3], Technology [4]

By Aine Cryts [5]

Physician practices can learn from Equifax's security breach by asking the right questions. Here are a few to ask their vendor.

Source: Physicians Practice

"Are you installing the latest security patches?"

That's one of the first questions physician practices should be asking their EHR vendors, says Gerard Nussbaum, principal at Zarach Associates, a Chicago-based healthcare consulting firm. He's taking his cue from recent news about the security breach at Equifax, which exposed 146 million Americans' financial and personal information. The company's CEO lost his job, as did other executives—and the publicly-traded company's stock was dealt a blow after news hit of the security breach. Before Congress in September, former Equifax CEO Richard Smith traced the vulnerability to the failure of a single employee to install and test a patch for a web application.

Here are five other things physician practices must ask their EHR vendors about their security breach plans:

**Policies and procedures.** Jim Kelton, managing principal at Costa Mesa, Calif-based Altius Information Technologies, says practices need to ask vendors about their policies and procedures in the event of a security breach — and it's also a good time to do that assessment internally, he adds. HIPAA requires that practices conduct a risk analysis evaluation of all their service providers to ensure the protection of patients' health information, points out Nussbaum.

**Security audit.** He also recommends that physician practices ask vendors for their latest security audit, which is often done by a third-party organization, such as a certified public accounting firm. Kelton says physician practices need to review the security audit in detail to determine any possible security risks and ask hard questions about the vendor's remediation plan in the face of those risks. For example, if the vendor says a high-level risk won't be addressed for 18 months, the practice needs to ask why.

**Financial resources.** In addition to trusting their EHR vendor, he says physician practices need to know their vendor can invest in resolving any security breaches. Specifically, practices should ask the vendor about the status of their cybersecurity coverage. Good follow-up questions include: What level of coverage does the vendor have? Are the premiums paid in full?

**Current terms and conditions.** Nussbaum points out that most vendors have the right to update the terms and conditions of their agreements with physician practices, which means someone at your practice has to proactively seek out the company's terms and conditions online and print and save them on a regular basis.

**Financial responsibility for breach.** Kelton says practices also need to know in advance who's paying for patients' free credit reports. Is that at the vendor's expense or is the practice responsible for those fees?

One of the biggest challenges with preventing security breaches at physician practices is there's no on-site expert on security and technology, says Nussbaum. That's why you need an in-house expert who can ask your EHR vendor the tough questions about their plans if the firm is ever hit by a security breach.

Source URL: http://www.physicianspractice.com/ehr/6-things-ask-your-ehr-vendor-about-security

Links: