Codify
BY AAPC

Health Information Compliance Alert

Cybersecurity: Combat Data Breaches in 2019 with These Expert Tips

Hint: There's more to a risk analysis than an EHR check-up.

If you haven't analyzed and updated your HIPAA compliance plan recently, now is a good time to get your ducks in a row for the new year.

Myth: Some small practices think that doing an annual risk analysis is not required.

Reality: According to the HIPAA Security Rule, that's not true. If you are a covered entity (CE), you are required to perform a risk analysis, clear and simple. "In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis," cautions the HHS Office of the National Coordinator for Health Information Technology (ONC) in its "Top 10 Myths of Security Risk Analysis" online resource.

"Covered entities and business associates should conduct an accurate and thorough risk analysis at least annually," advises **Jen Stone, MSCIS, CISSP, QSA,** a security analyst with **Security Metrics** in Orem, Utah. However, the reality is that many practices don't, and they may not even know how to start the process.

"Most organizations cannot meet the standards of the HIPAA Security Rule for a risk analysis without help from a third party that specializes in performing risk analyses," acknowledges Stone. "Risk analysis is not a skill set you can reasonably expect your IT team to have."

Review the 3 Biggest Breaches of 2018

Data breaches rocked the healthcare universe in 2018 as the stakes continued to rise due to cybersecurity issues. The loss of electronic protected health information (ePHI) came in all shapes and sizes with healthcare providers and organizations, both big and small, being impacted. But, three CEs experienced HIPAA breaches involving more than a million individuals each - and what's more, the HHS Office for Civil Rights (OCR) is still adding incidents to its breach portal for the year.

Here's a short overview of the three biggest losses of ePHI in 2018:

1. Business associate: North Carolina-based **AccuDoc Solutions, Inc. (AccuDoc)** in coordination with **Atrium Health** were victims of a cyber attack to their network servers. "Following an extensive forensics review, it appears that an unauthorized third party gained access to AccuDoc's databases between September 22, 2018 and September 29, 2018," noted an Atrium Health announcement on the breach. According to the OCR breach portal, 2,652,537 individuals were affected.

2. Health plan: Due to a coding issue or "security flaw" in the **Employees Retirement System of Texas (ERS)** "password-protected portal called ERS OnLine," beneficiaries were able to view other patients' ePHI and health plan information in addition to their own, revealed an ERS brief on the incident. ERS OnLine remained compromised from Jan. 1, 2018 to August 17, 2018, and 1,248,263 individuals' data was impacted.

3. Provider: Between March and April of 2018, employees at **Iowa Health System (UnityPoint Health)** were part of a social engineering scheme, initiated through email, declared the organization's notice of breach. According to the Unity Health release, forensic evidence showed that 1,421,107 individuals' ePHI was compromised, probably for financial gain.

Resolve Your Issues Now, Avert a Breach Later

Whether you service 500 patients or 5 million, you must perform a risk analysis and follow through on your HIPAA

compliance problems. Major setbacks this year involved the lack of policies and procedures, proper security and incident response protocols, staff education, and lack of encryption on devices and workstations.

Consider these expert tips from Stone as you go about managing your practice risks in 2019:

Utilize enhanced tools to best identify risks: "As part of the risk analysis, use results of automated tools, such as network-layer vulnerability scans and application-layer code security scans, to give you a reality check on the state of the systems in your ePHI environment," Stone says.

Ask for the information: "As a covered entity [CE], if you're trusting someone else to securely handle ePHI storage and transmission, asking for vulnerability scan results and [penetration test] pentest reports is a good way to ensure they protect your patients' information," Stone stresses. "Your business associate might think their code is secure, but can they show you that they have limited vulnerabilities in their systems with a third-party report?"

Implement from the results: "Use the risk analysis to implement or evaluate and modify your risk management plan," recommends Stone. "This plan is one way your IT team can prioritize work to strengthen the security stance of your organization from year to year."