Codify
BY AAPC

Health Information Compliance Alert

Security Rule: Debunk 10 Myths About HIPAA Security Compliance

Why cybersecurity doesn't trump physical security.

Misinformation and myths abound when it comes to healthcare data security. And although there is no way to protect your data 100 percent of the time, you can help to plug your organization's security holes by dispelling these common HIPAA myths.

1. Are Small Providers Less Vulnerable to Hacking?

Myth: Your healthcare organization is too small to be hacked.

Reality: "Even small healthcare companies get hacked," warned **Thomas Lewis** in a June 10 blog posting for **LBMC Security & Risk Services.** "In fact, some hackers prefer smaller organizations because they understand that they can be easier targets."

And if a hacking incident leads to a HIPAA breach, the size of your organization won't protect you from a government audit and potential sanctions, Lewis cautioned. The **HHS Office for Civil Rights** (OCR) will investigate organizations of any size when they suffer a data breach.

Caveat: But the OCR does take into consideration your organization's size, as well as your budget and whether you have limited resources, Lewis noted. "As long as you've documented why you've made the choices you have, OCR will take this into consideration, but in all cases, you need to make sure you are meeting the HIPAA standards."

2. Are Small Providers Exempt from Security Risk Analyses?

Myth: Performing the Security Risk Analysis is optional for small providers.

Reality: All providers not matter how big or small that handle protected health information (PHI) must perform a risk analysis, according to Seattle-based **Allpoint Compliance Solutions LLC** (ACS). There is no specific risk analysis format that you must follow, but you must address all three areas: administrative, physical, and technical.

3. Is Physical Security Not as Big of a Risk as Cybersecurity?

Myth: Hacking presents a much higher risk of a data breach than physical security problems.

Reality: This is one of the biggest myths when it comes to healthcare security compliance, Lewis said. "Data can be stolen in many ways, not just over a compromised network."

"Hospitals and other large clinical settings are targets of opportunity for thieves looking for personal information," Lewis warned. "Because these facilities are built for public access, protecting the data inside is not their primary objective."

Best bet: Prioritize strengthening physical security controls and network security, including "preventing unauthorized physical access to secure areas as well as preventing outright physical theft," Lewis advised.

4. Does Installing an EHR-Compliant System Satisfy Security Compliance?

Myth: Installing and using an electronic health record (EHR)-compliant system fulfills the security compliance requirements.

Reality: Using an EHR system that's HIPAA-compliant doesn't necessarily take care of all your security issues, ACS said. And your risk analysis should address all aspects of your system, not just the information contained in your EHR software.

5. Are Your Existing Controls Strict Enough?

Myth: Your existing security controls are strong enough.

Reality: "Sometimes we rely on our intuition to gauge the strength of our security controls," Lewis said. "Unfortunately, sometimes our intuition isn't enough to keep us secure or meet compliance mandates."

You organization must have security controls rigorous enough to both address your security risks and be HIPAA-compliant, Lewis noted. Make sure your security controls for your general business operations at least meet HIPAA standards for your network monitoring, access controls and employee training.

The best way to determine whether your existing security controls are strict enough is to conduct a risk assessment, Lewis recommended. Perform a "technical assessment of your security risks through activities like vulnerability scans or penetration tests, an analysis of the various threats, vulnerabilities and safeguards, as well as an assessment of how you stand against the HIPAA requirements related to Privacy, Security, and Data Breach Reporting."

6. Can You Rely on Your EHR Vendor?

Myth: Your EHR vendor is responsible for taking care of your security compliance.

Reality: If you think that your EHR vendor took care of everything you need to do about security, you're wrong, according to ACS. "Your vendor may be able to provide information, assistance and training, but [it's] not responsible for making [its] products compliant with HIPAA it is solely the responsibility of the entity to have a complete risk analysis conducted."

7. No Past Breaches, No Problem Right?

Myth: You've never had a breach before, so you don't need to worry so much.

Reality: "If you haven't had a breach, you may be thinking your controls are working," Lewis noted. "That could be the case, but it might not be. Why take the risk?"

The fact that you haven't had a breach simply means that you've dodged that proverbial bullet until now. "Consider yourself lucky, but don't fail to review and adjust security protocols to adequately protect healthcare data," Lewis said.

8. Can You Use a Checklist for the Risk Analysis?

Myth: A checklist will suffice for the security risk analysis.

Reality: Although you can use a checklist as a tool to help in your risk analysis, relying solely on a checklist will fall short of the comprehensive and clear documentation on what risks exist and how you're addressing those risks, ACS noted.

9. Is HIPAA Compliance Really Worth the Expense?

Myth: HIPAA compliance is too expensive.

Reality: "Yes, compliance costs some money, but not being compliant can lead to a huge fine from the federal government and loss of customer trust, not to mention loss of customers altogether," Lewis warned. "Plus, the notion that there needs to be a big technology spend on healthcare security compliance does not always hold true."

In many cases, healthcare organizations "have at least the basic tools already in place and the additional costs will be for administering security programs and compliance strategies," Lewis noted.

10. Do You Need to Perform a Risk Analysis More than Once?

Myth: You need to perform a risk analysis only once.

Reality: "Full HIPAA compliance requires that you must review, correct, modify and update security protections," ACS stated. "This can only be done by routinely reviewing systems in place and making changes when appropriate."