UNDERSTANDING HIPAA

10 Biggest Myths of HIPAA Risk Assessments

We've heard the stories about electronic protected health information (ePHI) being misused or released to the public. But did you know that mere lack of protection itself can put you in violation of the Health Insurance Portability and Accountability Act (HIPAA)?

In 2013, Idaho State University agreed to pay $400,000 to the U.S. Department of Health and Human Services (HHS) because of a disabled firewall on a server that contained the ePHI of over 17,000 patients.

Even though the information was never misused or made public, simply having a disabled firewall was enough to constitute a HIPAA violation and subject the school to steep fines.

Although HIPAA risk assessments have been required since the law's implementation, surprisingly few healthcare facilities complete them. Some smaller organizations can fill the requirement with a self-assessment; but even in such a case, it's best to have a trained professional conduct an assessment on a regular basis.

HealthIT.gov, a site dedicated to helping health care providers better manage, share and secure ePHI, has identified the following 10 biggest myths of HIPAA risk assessments and explained the truth behind them. Read on for the truth about how to protect your ePHI—and your organization.

At James Moore & Co., we've been providing technology services for over 25 years. Our firm is a Microsoft Gold partner, and the members of our dedicated Technology Solutions Consulting Team combine for decades of experience with a wide range of technical skills including:

- Security
- Single and multiple location network design
- Data backup and disaster recovery
- Business continuity
- Business process improvement
- New software or system implementation
- Performance monitoring and tuning
- Messaging and collaboration
- Cloud solutions
- Computer diagnostics and repair
- Operating systems support

Curtis McCallister, MCSE; MCTS: Exchange | Manager of Technology Solutions
888.387.6851 xt 2255 | Curtis.McCallister@jmcoit.com | www.jmco.com

James Moore
Technology Solutions Consultants

THE TOP 10 MYTHS OF SECURITY RISK ASSESMENT

1. The security risk assessment is optional for small providers.

False. All providers who are "covered entities" under HIPAA are required to perform a risk assessment. In addition, all providers who want to receive EHR incentive payments must conduct a risk assessment.

2. Simply installing a certified EHR fulfills the security risk assessment MU requirement.

False. Even with a certified EHR, you must perform a full security risk assessment. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.

3. My EHR vendor took care of everything I need to do about privacy and security.

False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk assessment conducted.

4. I have to outsource the security risk assessment.

False. It is possible for small practices to do risk assessment themselves using self-help tools. However, doing a thorough and professional risk assessment that will stand up to a compliance review will require expert knowledge obtained through services of an experienced outside professional.

5. A checklist will suffice for the risk assessment requirement.

False. Checklists can be useful tools, especially when starting a risk assessment, but they fall short of a professional security risk assessment including comprehensive documentation.

6. There is a specific risk assessment method that I must follow.

False. A risk assessment can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guidance assists organizations in identifying and implementing the most effective and appropriate safeguards to secure e-PHI.

7. My security risk assessment only needs to look at my EHR.

False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware, as well as software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data. Please see U.S. Department of Health and Human Services (HHS) guidance on remote use.

8. I only need to do a risk assessment once.

False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections. For more on reassessing your security practices, please see the Reassessing Your Security Practice in a Health IT Environment.

9. Before I attest for an EHR incentive program, I must fully mitigate all risks.

False. The EHR incentive program requires correcting any deficiencies (identified during the risk assessment) during the reporting period, as part of its risk management process.

10. Each year, I'll have to completely redo my security risk assessment.

False. Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior assessment for changes in risks. Under the Meaningful Use Programs, reviews are required for each EHR reporting period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP's year of participation in the program.

Curtis McCallister, MCSE; MCTS: Exchange | Manager of Technology Solutions
888.387.6851 xt 2255 | Curtis.McCallister@jmcoit.com | www.jmco.com

James Moore
Technology Solutions Consultants