PRACTICE PERFECT

INFORMATION TECHNOLOGY

EXTRA

CONTENT AVAILABLE

Perform a Security Risk Analysis: Top FAQs and Tips for Success

BY LESLIE BURLING-PHILLIPS, CONTRIBUTING WRITER
INTERVIEWING KYLE CHANG, CHARLES JARVIS, JULIA LEE, JD, OCS,
AND RONALD STERLING, CPA, MBA

As medical practices advance further and further into the world of digital information, the potential for data to become compromised escalates tremendously, whether due to a cyberattack, a lackadaisical employee, or poorly implemented office policies.

Failure to keep patient information safe from breaches in security can result in hefty HIPAA penalties of up to $50,000[1] per occurrence, as well as fines under the meaningful use program for electronic health records (EHR)—not to mention angry patients and sizable legal fees.

How well protected are your patients' records? Have you secured all possible loopholes? Fortunately, a thorough and ongoing risk analysis can help you identify and address any security vulnerabilities.

The Need for Risk Analysis

Why perform a risk analysis? "The protection of patient information is rapidly growing in importance—whether it is preventing the extraction of information from a network for marketing purposes or thwarting something more sinister such as identity theft," said Charles Jarvis, a senior manager for IT at the Coker Group, a health care advisory firm. "Data breaches and security hacks pose an ongoing, significant threat. Practices must take the appropriate steps to keep confidential patient information secure."

In order to preserve the privacy and security of patients' electronic protected health information (e-PHI), eligible professionals (EPs) must perform a security risk analysis during Stages 1 and 2 of meaningful use participation. This analysis is the first step toward compliance with the HIPAA Security Rule, and it forms the foundation upon which every practice should create and institute the applicable safeguards.

What is a security risk analysis? According to the Office of Civil Rights guidance on HIPAA, a security risk analysis is "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of e-PHI held by the organization. … This includes all e-PHI that an organization creates, receives, maintains, or transmits. All forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media," are also subject to the assessment

How to Perform Your Risk Analysis

The meaningful use risk analysis requirement poses challenges because there are no concrete steps for fulfilling this objective. Creating a one-size-fits-all approach to compliance is not feasible because practices vary in so many ways (e.g., staff size, number of locations, types of hardware connected to the network, etc.).

Here's why you should already know the basics. "Risk analysis is merely an extension of the HIPAA privacy rule. If you are already adhering to the HIPAA requirements, meaningful use compliance should come somewhat inherently," explained Ronald Sterling, CPA, MBA, of Sterling Solutions in Maryland.

Five areas to analyze. According to the Centers for Medicare & Medicaid Services (CMS), there are five areas that every practice must evaluate when conducting a security risk analysis:

- **Physical safeguards** (e.g., ensure that computer screens are shielded from unauthorized viewers)
- **Administrative safeguards** (e.g., enforce policies geared toward privacy protection)
- **Technical safeguards** (e.g., encrypt computer data)
- **Policies and procedures** (e.g., create written protocols for authorizing computer users)
- **Organizational requirements** (e.g.,

review and update business associate agreements)

Customize your risk analysis to reflect the needs of your practice. Using the five security areas defined by CMS, practices should 1) review their current security infrastructure, 2) identify potential areas of risk, and 3) eliminate the risk.

Designate a security officer within the practice. One person should be in charge of overseeing the security risk analysis and implementing suitable security safeguards. Throughout the year, the security officer will need to review policies, train staff, and ensure that patient information is kept secure. "At our practice, the information technology manager performs this role," said Julia Lee, JD, OCS, executive director of Ophthalmic Partners of Pennsylvania. "User activity is audited on an ongoing basis, and policy enforcement is a constant priority."

Allocate the necessary resources and time. Because risk analysis procedures are unique to each practice, the resources and time allocated to its performance will vary greatly.

Amend your analysis as needed. Regardless of practice size, however, risk assessment is an ongoing obligation. "Changes in infrastructure, technology, or staff, for instance, should immediately prompt a reevaluation of your risk—this is not a one-and-done endeavor," said Ms. Lee. Mr. Sterling elaborated: "Any time you have a change in your organization that could affect your risk profile [e.g., a new piece of equipment is added or a second location is opened], you must update your security risk assessment."

Resolve issues uncovered during the analysis. "The government expects providers to take action when a problem is identified. In fact, a primary focus of Stage 2 meaningful use audits is examining a practice's list of analysis recommendations to ascertain the progress it has made toward resolving those risk factors. Equally important, if a breach were to occur, any organization investigating that breach will immediately want to reference your risk assessment, find out what recommendations were made, and scrutinize how much progress was made toward remedying each issue," explained Kyle Chang, a senior manager of IT services at the Coker Group.

How to Avoid Problems

Keep hardware and software up to date. "Network devices that are not updated as needed become susceptible to malware, viruses, and intrusions. There is a tendency for practices to try to extend the usability of technology as long as possible, but this is counterproductive. While it may save some money in the short term, obsolete technology can expose a practice to a variety of security risks," said Mr. Chang, who recommended conducting a long-range needs assessment by anticipating future hardware and software requirements in conjunction with how much a practice's data are expected to grow.

Keep policies and procedures current. Your practice's employee handbook or policy and procedures should address data security and clearly define your staff's obligations to protect e-PHI. According to Ms. Lee, "This should include even the most basic rules of access like: Do not share your password. Do not use someone else's login. Each employee should have a unique login. When employees leave, old login credentials should be deleted. Always log out and lock your computer whenever you step away from your workstation." Further, "there should be a great deal of employee training and sensitivity with regard to proper data management," said Mr. Jarvis. "This will help ensure that when e-PHI is exchanged, all of the protections will be applied, which will reduce the opportunity for breaches."

Prepare for an audit. All documentation, including policies and procedures, should be kept in a "book of evidence" or "compliance binder," which documents how a practice is addressing security issues. This information should be readily accessible to the staff, both online and, in case the system is inoperable, in paper form. "This binder will act as a central repository for all items demonstrating MU [meaningful use] measure compliance—including the security risk analysis—and will be your primary source of information during an audit," said Ms. Lee.

Where Can I Get Help?

Vendor support is limited. Built-in protections from your EHR vendor are important, but they do not ensure compliance with the meaningful use requirement. "Actually, this is an impractical assumption because the compliance obligation encompasses much more than just your EHR system. Although vendors can incorporate endless protections, unless a practice utilizes these safeguards, they are of no use," Ms. Lee explained. Mr. Sterling agreed: "When we talk about certified EHR technology (CHERT), it simply means that the software has undergone an evaluation process and offers features that can be used to secure e-PHI under HIPAA security rules. The actual use of that system in an appropriate way is the responsibility of the health care organization, not the vendor. In fact, you could be using a CHERT and be completely noncompliant." ■

[1] www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html. Accessed Feb. 23, 2015.

[2] www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. Accessed Feb. 23, 2015.

***Kyle Chang** is senior manager of IT services at the Coker Group, Atlanta. Financial disclosure: Is employed by a consulting firm.*

***Charles Jarvis** is senior manager in the IT services division of the Coker Group, Atlanta. Financial disclosure: Is employed by a consulting firm.*

***Julia Lee, JD, OCS,** is executive director of Ophthalmic Partners of Pennsylvania, which has locations in Pennsylvania and New Jersey. Financial disclosure: Is a consultant for Alcon.*

***Ronald Sterling, CPA, MBA,** is principal consultant at Sterling Solutions, Silver Spring, Md. Financial disclosure: Is employed by a consulting firm.*

EXTRA *MORE ONLINE. For a list of helpful tools, tipsheets, guidebooks, and more, see this article online at www.eyenet.org.*