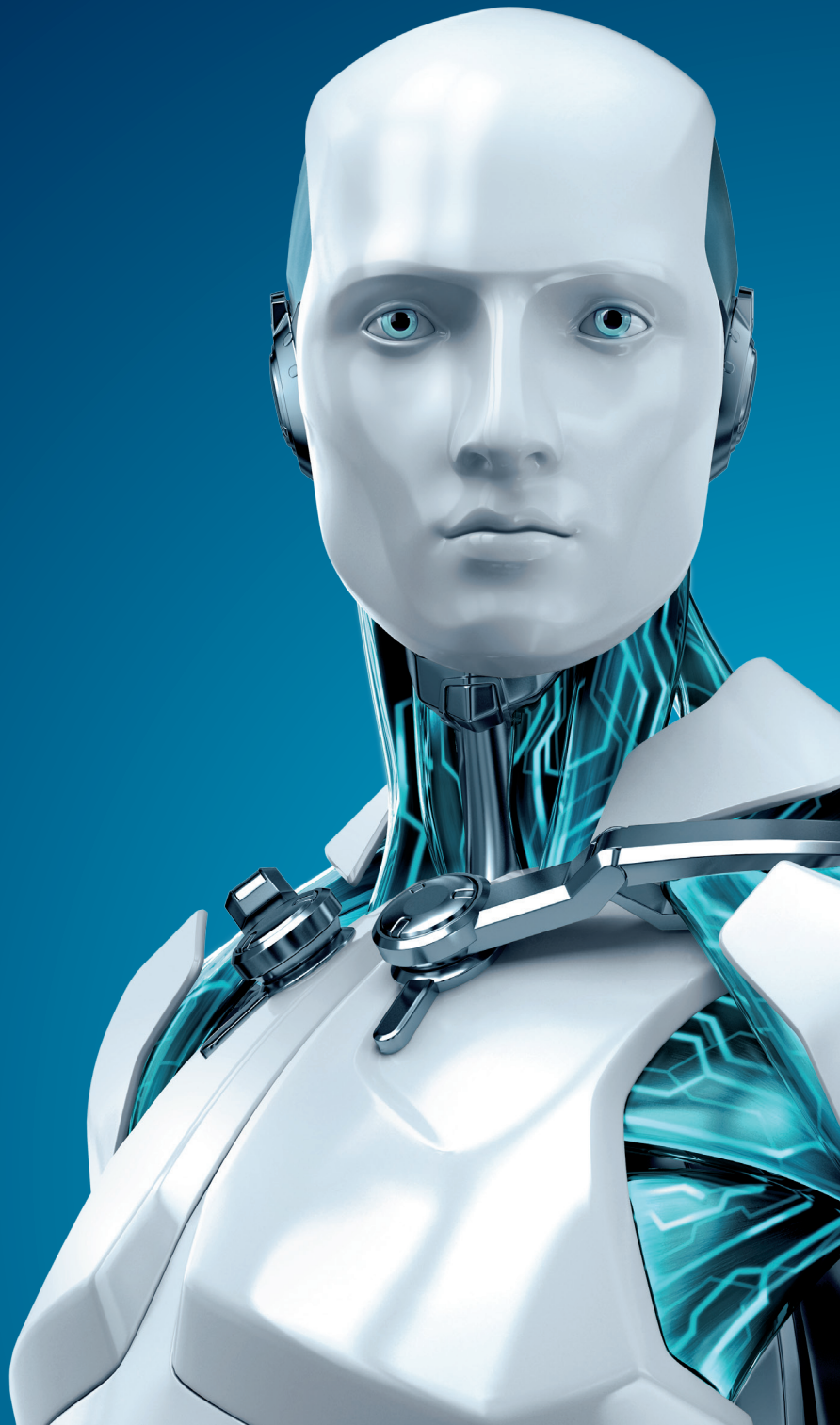
TECH BRIEF

Getting Started:
EHR Risk Assessment



ENJOY SAFER TECHNOLOGY™

GETTING STARTED WITH AN EHR RISK ASSESSMENT

Lysa Myers, ESET Security Researcher

Performing a risk assessment for safeguarding electronic patient health information (ePHI) is part of complying with HIPAA regulations. Such an assessment is also a meaningful use requirement of the Medicare and Medicaid electronic health record (EHR) Incentive Programs.

Unfortunately, risk assessment is not fully understood or implemented by some healthcare organizations, especially smaller facilities that lack dedicated IT or security staff. How do you proceed if your organization lacks the expertise? The answer to that question could easily fill volumes. However, the process has to start somewhere. Here is a basic description that covers the fundamentals, to help you steer your organization in the right direction. This brief concludes with a list of resources to help you take the next steps.

The Basics of a Risk Assessment

There are three basic steps. The time and effort they require depend upon the size and complexity of your organization. You may prefer to approach the effort using multiple passes over time, getting more in-depth with each iteration. This splits a huge project into something more manageable. You can then revisit to add depth and detail, and keep up with changes as they occur.

STEP 1: Identify your assets and transmission methods

The first step in any risk assessment is to identify and document the EHR assets in your organization. This encompasses anything that is used to input, store or transmit ePHI, including for example patient names, addresses, Social Security numbers, email addresses, fingerprints or photographic images. Remember that ePHI could end up in locations that you might not initially expect. Patient names and email or physical addresses are likely to be found in appointment information, and Social Security numbers might be included in billing and insurance records. The most likely places for ePHI to be stored include laptops, hard drives or servers, backups, cloud services, mobile devices, smart cards and other portable media. Be sure to not overlook web applications and non-Windows systems, such as medical devices, printers and scanners.

Of course, medical information is not static — it moves. Identify your transmission methods and consider all sources and destinations of information, including doctors, nurses, patients, insurance providers, backup services and cloud providers. These transmissions could take place via regular mail or email, text message, instant message, via the Web, or by Health Information Exchange, fax or network shares.

Transmission could also occur via applications for billing, patient management, prescription management or other functions. You can start identifying this information by looking at current and past projects, as well as at existing policies/procedures. It is also incredibly useful to consult IT and other staff, as they may be using methods that are not documented. If you are in a small clinic that has all its information on one machine, this step may go quite quickly. If you are assessing a larger organization, this will necessarily be more complex

and full of potential surprises. This is where a rolling risk assessment is particularly helpful: As your assets and methods of transmission evolve, you can note this in your documentation, so you do not have to restart the identification process each time you revisit the assessment.

STEP 2: Examine risks and vulnerabilities

Once you have identified your assets, you can begin to evaluate the risks and threats to them. It is important to consider not just cybercrime problems, but also any other human-made, natural or environmental troubles that could befall your systems. That includes the possibility of disgruntled employees or contractors as well as power outages and weather-related damage such as earthquakes or major storms. Such incidents could also lead to possible exposure of ePHI. Do not dismiss any possible calamity at this stage, no matter how far-fetched it seems; the requirement is not that you fully address every possibility, but rather that you consider them and the relative risk that they present. Like the identification of assets, this step needs regular updating, since known vulnerabilities change frequently. This step and the following one are also collectively known as Business Continuity Management (BCM) – which simply means ensuring that your business keeps running, even in the event of an emergency.

STEP 3: Assess the relative likelihood and impact of threats and vulnerabilities

Once all of the disastrous scenarios are listed, create a matrix that ranks them in terms of severity of impact and likelihood of occurrence. Some problems are minor, but likely to occur; others are more severe but unlikely. You will find it helpful to get multiple perspectives on the relative probability of threats, so consider enlisting outside experts for help at this stage.

Once you have documented all of the above, review the measures you already have in place to help avoid, mitigate or transfer risk – for example, anti-malware protection, encryption, firewalls and two-factor authentication. Are you missing any of these? What about cybersecurity insurance and employee education? Also, consider plans for testing and deploying software updates and patches on your machines, including mobile devices and embedded systems. Any gaps should be documented and then addressed. When considering the cost and effectiveness of the countermeasures to address gaps, it is important to balance this with the value of the asset being protected.

Next Steps

Once you have covered the basics described here, you can start with the resources below to more fully flesh out your assessment. Risk assessment is an iterative process that is an ongoing responsibility, rather than something you do once and consider complete. Business environments, the threat and vulnerability landscape – as well as defensive technologies – are all constantly changing.

Additional resources

- Internal Auditor article with more info on where to audit: http://www.theiia.org/intAuditor/itaudit/archives/2008/january/assessing-it-risks-in-the-health-care-industry/
- SMB Risk Assessment tool: http://www.healthit.gov/providers-professionals/security-risk-assessment
- Health and Human Services security and privacy training materials: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html
- Risk Assessment Frameworks: http://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment
- Computer Security Handbook (especially chapters 58, 59 and 62): http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118127064,subjectCd-AC03.html