Security Risk Analysis Tipsheet: Protecting Patients' Health Information

Conducting or reviewing a security risk analysis to meet the standards of Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule is included in the meaningful use requirements of the Medicare and Medicaid EHR Incentive Programs. Eligible professionals must conduct a security risk analysis in both Stage 1 and Stage 2 of meaningful use to ensure the privacy and security of their patients' protected health information:

Stage 1 and Stage 2 Meaningful Use Requirement: Protect Electronic Health Information		
Objective	**Measure**	**Description of HIPAA Requirement**
Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.	In Stage 1, eligible professionals must conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process. In Stage 2, eligible professionals need to meet the same security risk analysis requirements as Stage 1, but must also address the encryption/security of data at rest. *Note: a security risk analysis needs to be conducted during each reporting period for Stage 1 and Stage 2.*	Under the HIPAA Security Rule, you are required to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Once you have completed the risk analysis, you must take any additional "reasonable and appropriate" steps to reduce identified risks to reasonable and appropriate levels. (45 CFR 164.308(a)(1)(ii)).

This tipsheet[1] provides an overview of the security risk analysis requirement. Meaningful use does not impose new or expanded requirements on the HIPAA Security Rule, nor does it require specific use of every certification and standard that is included in certification of EHR technology. You can also find additional information and resources to assist you in learning more about the the HIPAA Security Rule through the the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

Performing a Security Risk Analysis

Today many patients' protected health information is stored electronically, so the risk of a breach of their e-PHI, or electronic protected health information, is very real.

To help you conduct a risk analysis that is right for your medical practice, OCR has issued Guidance on Risk Analysis.

[1] Content adapted from the HHS Office of the National Coordinator on Health Information Technology's Guide to Privacy and Security of Health Information

There is no single method or "best practice" that guarantees compliance, but most risk analysis and risk management processes have steps in common. Here are some considerations as you conduct your risk analysis:

- Review the existing security infrastructure in your medical practice against legal requirements and industry best practices
- Identify potential threats to patient privacy and security and assesses the impact on the confidentiality, integrity and availability of your e-PHI
- Prioritize risks based on the severity of their impact on your patients and practice

Create an Action Plan

Once you have completed these steps, create an action plan to safeguard the confidentiality, integrity and availability the e-PHI and make your practice better at protecting patients' health information.

Your action plan will involve a review of your electronic health information system to correct any processes that make your patients' information vulnerable. Make sure your analysis examines risks specific to your practice. For example, how do you store patient information—on an EHR system in your office, or on an Internet-based system? Each scenario carries different potential risks.

Your risk analysis may also reveal that you need to update your system software, change the workflow processes or storage methods, review and modify policies and procedures, schedule additional training for your staff, or take other necessary corrective action to eliminate identified security deficiency.

Protecting Patients' Electronic Information

Your security risk analysis will help you measure the impact of threats and vulnerabilities that pose a risk to the confidentiality, integrity and availability to your e-PHI. Once you have completed the risk analysis of your practice's facility and information technology, you will need to develop and implement safeguards to mitigate or lower the risks to your e-PHI. For example, if you want to assure continuous access to patient information, you may need to add a power surge protection strip to prevent damage to sensitive equipment from electric power surges, put the computer server in a locked room, and become meticulous about performing information system backups.

The Security Rule requires that you put into place reasonable and appropriate administrative, physical and technical safeguards to protect your patients' e-PHI. The Security Rule allows you to tailor security policies, procedures, and technologies for safeguarding e-PHI based on your medical practice's size, complexity, and capabilities—as well as its technical, hardware, and software infrastructure.

The following table shows some examples of some safeguards and processes you might put in place to mitigate security risks to your practice. These are only examples and should not be used as a comprehensive guide for mitigating security risks. You should put into place reasonable and appropriate administrative, physical and technical safeguards that are tailored to the size and complexity of your practice.

Security Areas to Consider		Examples of Potential Security Measures
Physical Safeguards	• Your facility and other places where patient data is accessed • Computer equipment • Portable devices	• Building alarm systems • Locked offices • Screens shielded from secondary viewers
Administrative Safeguards	• Designated security officer • Workforce training and oversight • Controlling information access • Periodic security reassessment	• Staff training • Monthly review of user activities • Policy enforcement
Technical Safeguards	• Controls on access to EHR • Use of audit logs to monitor users and other EHR activities • Measures that keep electronic patient data from improper changes • Secure, authorized electronic exchanges of patient information	• Secure passwords • Backing-up data • Virus checks • Data encryption
Policies & Procedures	• Written policies and procedures to assure HIPAA security compliance • Documentation of security measures	• Written protocols on authorizing users • Record retention
Organizational Requirements	• Business associate agreements	• Plan for identifying and managing vendors who access, create or store PHI • Agreement review and updates

Myths and Facts

The following table addresses common myths about conducting a risk analysis, and provides facts and tips that can help you structure your risk analysis process.

Seurity Risk Analysis Myths and Facts	
Myth	**Fact**
The security risk analysis is optional for small providers.	False. All providers who are "covered entities" under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.
Simply installing a certified EHR fulfills the security risk analysis MU requirement.	False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.
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 analysis conducted.

Seurity Risk Analysis Myths and Facts	
Myth	**Fact**
I have to outsource the security risk analysis.	False. It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.
A checklist will suffice for the risk analysis requirement.	False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.
There is a specific risk analysis method that I must follow.	False. A risk analysis 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.
My security risk analysis 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 and 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.
I only need to do a risk analysis once.	False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections.
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 analysis) according to the timeline established in the provider's risk management process, not the date the provider chooses to submit meaningful use attestation. The timeline needs to meet the requirements under 45 CFR 164.308(a)(1), including the requirement to "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [45 CFR]§164.306(a)."
Each year, I'll have to completely redo my security risk analysis.	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 analysis for changes in risks. Under meaningful use, 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.

For more information, including a ten-step plan for health information privacy and security, review ONC's Guide to Privacy and Security of Health Information, or visit OCR's webpage.

Revised: December 2013