Protect Electronic Health Information

Protect electronic health information; these four words continue to cause frustration and confusion for many health care providers and hospitals operating today. Starting with Stage 1 Meaningful Use (MU), protecting electronic health information was a measure, still a measure with Stage 2 MU, and will most likely always be a measure in the MU program. To help limit any frustration and/or confusion, please review some of the key components to meeting this measure and achieving MU:

The Basics

The Objective:
Protect electronic health information created or maintained by the certified electronic health record (EHR) technology through the implementation of appropriate technical capabilities.

The Measure:
In Stage 1, eligible professionals and eligible hospitals 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 and eligible hospitals 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 or reviewed during each reporting period for Stage 1 and Stage 2.

Performing a Security Risk Analysis
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 assess 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 of 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 deficiencies.

The following table is from CMS Publication 11/22/2013

Security 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.
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.
Security Risk Analysis Myths and Facts	
Myth	**Fact**
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 on protecting electronic health information, performing a security risk analysis, and other services provided by the WTxHITREC, please call (806) 743-7960, email info@wtxhitrec.org or visit www.wtxhitrec.org.

*Source: CMS Publication 11/22/2013