EHR 2.0
Ensure HIPAA Compliance

MEANINGFUL USE SECURITY RISK ANALYSIS FOR STAGE 2

9/17/2015

Conduct an Effective Security Risk Analysis which will withstand CMS/OIG audit

There is a lot of confusion and challenges around conducting an effective security risk analysis to fulfill the core objective requirements of Meaningful Use (MU) by eligible professionals and hospitals. The purpose of this whitepaper is to provide an initial overview and clarify the requirements of security risk analysis for MU.

Meaningful Use Security Risk Analysis for Stage 2

CONDUCT AN EFFECTIVE SECURITY RISK ANALYSIS WHICH WILL WITHSTAND CMS/OIG AUDIT

CMS Attestation Requirement

Center for Medicare and Medicaid Services' (CMS) core measure for protecting electronic health information requires Protected Health Information (PHI) created and/or maintained by EHR systems to be secured through the implementation of appropriate technical capabilities. In order to implement appropriate technical controls, eligible professionals and hospitals need to conduct a security risk analysis in accordance with the requirements under HIPAA security rule 45 CFR 164.308(a)(1), apply security updates as necessary, and correct identified security deficiencies as part of their risk management process.

Scope

The scope of risk analysis encompassed by the HIPAA security rule includes the potential risks and vulnerabilities to the confidentiality, availability, and integrity of all electronic PHI that an organization creates, receives, maintains, or transmits. This applies to e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards, other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation, as well as complex networks connected between multiple locations. Thus, an organization's risk analysis should take into account all of its e-PHI, regardless of the particular electronic medium in which it is created, received, maintained, or transmitted or the source or location of its e-PHI.

Where to start

RESOURCES

- ✓ FAQ
- ✓ CMS Resources
- ✓ NIST Guidelines

Call: 866-276 8309

E-mail: info@ehr20.com

Web: ehr20.com

Meaningful Use Security Risk Analysis for Stage 2

CONDUCT AN EFFECTIVE SECURITY RISK ANALYSIS WHICH WILL WITHSTAND CMS/OIG AUDIT

Conducting a Security Risk Analysis

1. Identify and document potential threats and vulnerabilities
Healthcare organizations must identify and document reasonably anticipated threats to e-PHI, which are often unique to the circumstances of their environment. Organizations must also identify and document vulnerabilities, which if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI.

2. Assess current security measures
Organizations should assess and document the security measures used to safeguard e-PHI, whether measures required by the security rule are already in place, and if current security measures are configured and used properly. The security measures implemented to reduce risk will vary among organizations. For example, small practices tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard ePHI, which allows them more control within their environment. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability, and integrity of e-PHI in a small organization may differ from those necessary for large organizations.

3. Determine the likelihood of threat occurrence
The HIPAA security rule requires organizations to take into account the probability of potential risks to e-PHI. The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires additional protection against because they are "reasonably anticipated." The output of this evaluation should include documentation of all threat and vulnerability combinations, with the respective estimates of likelihood these may impact the confidentiality, availability, and integrity of e-PHI of an organization.

4. Determine the potential impact of threat occurrence
The rule also requires consideration of the "criticality" or impact of potential risks to confidentiality, integrity, and availability of e-PHI. An organization must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. An entity may use either a qualitative or quantitative method or a combination to measure the impact on the organization. The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability, and integrity of e-PHI within an organization.

5. Determine the Level of Risk
Organizations should assign risk levels for all threats and vulnerabilities identified during risk analysis. The level of risk may be determined by analyzing the likelihood of threat occurrence and resulting impact of threat occurrence. The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level.

TOOLKIT

Our risk assessment toolkit covers the following three key areas that healthcare organizations need to comply with:

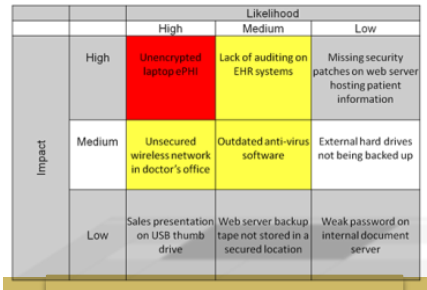
1) ePHI Inventory
2) Risk Assessment
3) Prioritization
4) Action Plans

Call: 866-276 8309

E-mail:

info@ehr20.com

Web: ehr20.com



OUR SERVICES

EHR 2.0 specializes in security risk assessments, customized for individual organizations:

- Security Risk Analysis Consulting
- Prioritization and Mitigation of Risks
- Action Plans
- MU Attestation

Call: 866-276 8309

E-mail: info@ehr20.com

Web: ehr20.com

6. Prioritize, Action Plans and finalize documentation

Identified risks need to be prioritized to be managed effectively, as every health organization has limited resources available. The Security Rule requires the risk analysis to be documented but does not require a specific format (See 45 C.F.R. § 164.316(b) (1)). The risk analysis documentation should serve as a direct guide to the risk management process.

Periodic Review and Updates to the Risk Assessment

The risk analysis process should be ongoing, in order for an entity to update and document its security measures "as needed," which the rule requires. The frequency of performance will vary among organizations. A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. For example, if the covered entity has experienced a security incident, change in ownership, turnover in key staff or management, or is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure the e-PHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against evolving threats or vulnerabilities, a changing business environment, or the introduction of new technology, then the entity must determine if additional security measures are needed.

Summary

The primary goal of security risk analysis for meaningful use is to identify the key technical vulnerabilities in the electronic Protected Health Information (ePHI) and EHR systems environment. An EHR 2.0 risk analysis service ensures you identify the key technical risks in high priority areas and develop a program to mitigate the risks identified. Attestation of the risk analysis is required every year to receive Center for Medicaid and Medicare Services (CMS) incentive payments. Our consulting team at EHR 2.0 takes a systematic approach in meeting this requirement. Our members' decades of experience in successfully conducting technical risk analysis, drawing guidance from various authoritative sources and our best practices-based online toolkit platform, help not only meet the core objective requirements but also secure your practice's PHI. Risk analysis is the first step in HIPAA security rule compliance efforts and is an ongoing process to provide the practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of ePHI.

Learn more at ehr20.com