EHR 2.0
THE HIPAA COMPLIANCE EXPERTS

# SECURITY RISK ANALYSIS FOR HIPAA COMPLIANCE

An EHR 2.0 White Paper
April 2016

## How to Conduct an Effective Security Risk Analysis which will withstand an HHS/OCR audit

There continues to be confusion and challenges around conducting an effective security risk analysis to fulfill the core objective requirements of HIPAA compliance by physician practices and hospitals. The purpose of this whitepaper is to provide an initial overview and clarify the requirements for security risk analysis for HIPAA.

# Security Risk Analysis for HIPAA Compliance

## HOW TO CONDUCT AN EFFECTIVE SECURITY RISK ANALYSIS WHICH WILL WITHSTAND AN HHS/OCR AUDIT

### HIPAA Security Analysis Requirement

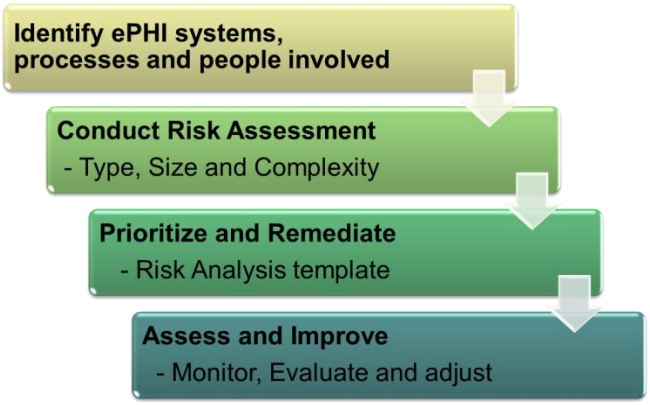
Covered Entities and Business Associates who maintain Protected Health Information(PHI) must conduct a security risk analysis in accordance with the requirements under HIPAA security rule 45 CFR 164.308(a)(1), apply security updates as necessary, and correct identified security deficiencies as part of their risk management process. Conducting a thorough risk analysis is the first step in identifying and implementing safeguards that comply with HIPAA regulations, and carry out the standards and implementation specifications in the Security Rule. A risk analysis is foundational and must be understood in detail before specifically building a plan that will best protect electronic health information.

### Scope

The scope of risk analysis that the HIPAA security rule encompasses 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 includes ePHI in all forms of electronic media; hard drives, floppy disks, CDs, DVDs, smart cards, or 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 ePHI, regardless of the particular electronic medium in which it is created, received, maintained, or transmitted or the source or location of its ePHI.

### Where to start

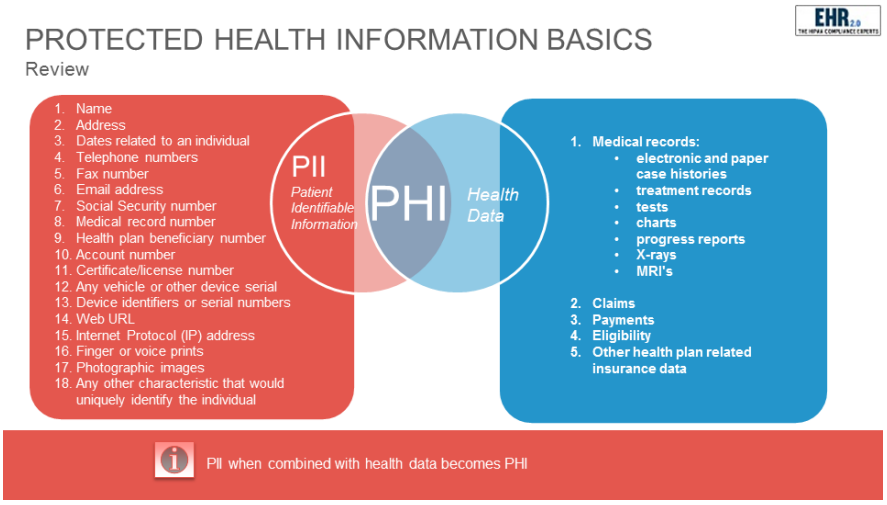
Given the complexity of the HIPAA privacy, security and breach regulations, it is important to determine what organizations need to do to comply. A key preliminary step toward the goal of implementation is conducting a comprehensive HIPAA security risk assessment. This chart below describes a phased risk-assessment approach that institutions of any size can follow.



## HOW TO CONDUCT AN EFFECTIVE SECURITY RISK ANALYSIS WHICH WILL WITHSTAND AN HHS/OCR AUDIT

### What is PHI?

Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.




- Past, present, or future physical or mental condition of an individual
- Provision of health care to an individual
- Past, present or future payment for the provision of health care to an individual

Personally Identifiable Information when combined with clinical/medical records becomes PHI.

Also, health information by itself without the 18 identifiers is not considered to be PHI. For example, a dataset of vital signs by themselves do not constitute protected health information. However, if the vital signs dataset includes medical record numbers, then the entire dataset must be protected since it contains an identifier.

## CONDUCTING A SECURITY RISK ANALYSIS

**1. Identify and document potential threats and vulnerabilities**

Healthcare organizations must identify and document reasonably anticipated threats to ePHI. Organizations may identify different threats that are 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 unauthorized access to or disclosure of ePHI.

**2. Assess current security measures**

Organizations should assess and document the security measures an entity uses to safeguard ePHI. Whether security 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 more control within their environment; 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. As a result, the appropriate security

measures that reduce the likelihood of risk to the confidentiality, availability, and integrity of ePHI in a small organization may differ from those that are appropriate in 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 ePHI. The results of this assessment, combined with the initial list of threats, will influence the determination of which threats and or vulnerabilities the Rule requires protection against because they are "reasonably anticipated." The output of this part should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability, and integrity of ePHI of an organization.

**4. Determine the potential impact of threat occurrence**

This rule requires consideration of the "criticality," or impact, of potential risks to confidentiality, integrity, and availability of ePHI. 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 of the two methods 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 ePHI within an organization.

**5. Determine the Level of Risk**

Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels. The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level.

**6. Prioritize and finalize documentation**

Identified risks need to be prioritized in order to be managed effectively, as every health organization struggles to focus on priorities. 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 is a direct input 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, practices should conduct continuous risk analysis to identify when updates are needed. The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among organizations. Some organizations may perform these processes annually or as needed (e.g., bi-annual or every 3 years), depending on circumstances of their environment. 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, has had 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 ePHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with 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 a security risk analysis for HIPAA is to identify the key technical vulnerabilities in the electronic Protected Health Information (ePHI) and EHR systems environment. A thorough risk analysis ensures you identify the key technical risks in your areas and develop a program to mitigate the risks identified. Updates to risk analysis is required every year to ensure organizations comply with HIPAA annual evaluation requirements. A very systematic approach in meeting this requirement ensures practices can handle any potential OCR/HHS audit documentation requests. A complex PHI workflow requires conducting technical risk analysis, drawing guidance from various authoritative sources and security best practices to not only meet the compliance requirements, but also to secure your practice. Risk analysis is the first step in healthcare practices' HIPAA security rule compliance efforts as well. Risk analysis is an ongoing process that should provide the practice with a detailed understanding of any risks to the confidentiality, integrity, and availability of ePHI.

## EHR 2.0 - Your HIPAA Compliance Partner

EHR 2.0 is a Health IT Consulting company specializing with assisting healthcare organizations and business associates comply with HIPAA & HITECH compliance requirements.

We offer the following services:

- Meaningful Use Security Risk Analysis
- Meaningful Use Attestation Services
- HIPAA/HITECH Compliance Assurance
- HIPAA Compliance Maintenance Program
- Business Associate Compliance
- CMS/HHS/OCR/OIG Audit Advisory Services
- Staff Training on HIPAA Security Awareness
- PQRS Attestation Services

Our Consultants are security experts, well versed with HIPAA laws (Chapter 45 of the Code of Federal Regulations Section 164.308(a)(1) and the Meaningful Use Core measure #15 mandatory ruling.
We use the standards and guidelines set by the National Institute of Standards & Technology (NIST) to conduct the Analysis. Our consultants are certified in security and hold certifications in CISSP, CISM, CISA.

Our one-stop HIPAA Compliance solutions helps secure electronic patient data, saves time and money and bring peace of mind in case of an audit. EHR 2.0 will ensure your organization is fully HIPAA compliant, and stays compliant throughout the year.

Visit www.ehr20.com for more information.