# Security Risk Analysis: Step One of an Effective Cybersecurity Program

**By Loretta Verbeck, MS, FACMPE, CHC**

Cybersecurity is a topic that physicians and their staff cannot ignore. Ransomware, data breaches, distributed denial of service (DDoS) attacks, and email fraud are just a few of the cybersecurity issues that can cause financial and reputational damage to any organization. In healthcare, the impact of a cyber-attack goes beyond financial and reputational damage. It can also disrupt the ability to provide patient care. This is why healthcare organizations must implement an effective cybersecurity program.

The HIPAA Security Rule requires covered entities, which includes nearly all healthcare organizations, to protect the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that is created, received, maintained, or transmitted by the entity. The Rule includes administrative, physical, and technical standards and implementation specifications that are either required or addressable. At a minimum, HIPAA covered entities must conduct a risk analysis by assessing their current risks, security measures already in place, and any remaining gaps that need to be addressed.

The first standard under administrative safeguards is the security management process which includes risk analysis and risk management. These two implementation specifications are required by the Security Rule and, if conducted and implemented appropriately, can reduce the risk of a successful cyber-attack. Unfortunately, based on findings from the 2016-2017 HIPAA Audits Industry Report, released in December 2020, “most covered entities and business associates failed to implement the HIPAA Security Rule requirements for risk analysis and risk management.” Lack of an accurate and thorough risk analysis is also one of the most cited deficiencies in enforcement action taken by the Department of Health and Human Services (HHS).

The Security Rule does not require a specific risk analysis methodology, but guidance has been developed by the Centers for Medicare and Medicaid Services (CMS) in large part based on the National Institute of Standards and Technology (NIST) 800 Series of Special Publications (SP), specifically, SP 800-30 - Risk Management Guide for Information Technology Systems. Depending on the size of the practice, the complexity of systems containing ePHI, and the technical expertise of the workforce, it may be necessary to outsource the risk analysis process. There are a number of third-party vendors that can assist covered entities with this process. However, even if the risk analysis is performed by a third-party, the covered entity is ultimately responsible for ensuring that it is accurate and thorough.

The following steps are summarized from the CMS guidance to help medical practices conduct their own internal risk analysis or determine if an outsourced risk analysis is sufficient to meet the Security Rule criteria.

1. **Identify the Scope & Gather Data**

   The scope of an accurate and thorough risk analysis must include **all** ePHI that is created, received, maintained, or transmitted. This means thinking beyond the electronic health record and billing system to develop a proper ePHI inventory. There are many places and systems that are overlooked by practices when conducting a risk analysis. That is why it is important to include the entire organization in the process. This can be accomplished by interviewing workforce members, using surveys to inquire how ePHI is being shared internally and externally, and identifying systems and devices used to create, send, or receive ePHI.

Some examples of systems that could be left out of a risk analysis are telephone systems using voice over internet protocol (VoIP), email applications, mobile devices used by workforce members, portable storage devices, and cloud storage. The scope and method of gathering data must be documented regardless of the size of the organization. If the organization is large, with several departments or facilities, the scope must be enterprise-wide.

2. **Identify Potential Threats & Vulnerabilities**

   Once an ePHI inventory has been developed, the next step is to identify the potential threats and vulnerabilities to the confidentiality, integrity, and availability of that ePHI. A threat is the potential for a specific vulnerability to be triggered or exploited. Threats can be natural (floods, earthquakes, tornados), human (intentional or unintentional actions by people), or environmental (power failure, pollution, chemicals). A vulnerability is a flaw or weakness in systems or processes that could result in a security breach or a violation of a security policy if triggered or exploited. Threats and vulnerabilities must be documented.

3. **Assess Current Security Measures**

   Even when a risk analysis is being conducted for the first time, it is likely that the practice has some security measures already in place. In this step, current security measures should be documented. Security measures can be technical (automatic logoff, encryption) or non-technical (policies and procedures). Security measures will vary with the size of the organization. The goal of this step in the risk analysis process is to minimize or eliminate risks to ePHI.

4. **Determining Level of Risk**

   Using the ePHI inventory, along with identified threats and vulnerabilities, and security measures already in place, the practice can now determine the level of risk to ePHI. The level of risk is determined by the threat's likelihood of occurrence and the impact on ePHI should the threat occur. The purpose of determining the risk level of each threat is to prioritize efforts to reduce risks to a reasonable level.

Each threat should be given a likelihood of occurrence. This can be as simple as rating each threat as low, medium, or high. Next, determine the impact to the confidentiality, integrity, or availability of ePHI if the threat does occur. For example, if the practice is in a flood zone, the likelihood that a flood (threat) could occur is high. The impact on ePHI if the practice does not have an offsite backup (vulnerability/lack of security measure) will also be high. The combination of high likelihood and high impact results in high risk. On the other hand, if the practice has an offsite backup that can be restored if systems storing ePHI are damaged in a flood, the impact to ePHI would be low. The combination of high likelihood and low impact results in a low level of risk.

5. **Identify Security Measures and Finalize Documentation**

   Now that risk levels have been assigned, it is time to determine the actions that must take place to reduce risks to reasonable and appropriate levels. When choosing safeguards, practices should consider the regulatory requirements of the Security Rule's standards and implementation specifications and any existing security policies and procedures. Once safeguards have been identified, documentation of the results can be finalized.

The Security Rule does not require a specific format for documentation, but it should be done in a way that is useful for the practice. For example, a spreadsheet that lists the risk analysis process, results of each step, and initial identification of security measures would serve the purpose of documenting the risk analysis and provide a starting point for the risk management process.

Following the Security Rule requirement to conduct a risk analysis is the first step of an effective cybersecurity program because it puts the spotlight on areas that pose the most significant risks to your practice. Once the risks are identified, action can be taken to reduce those risks to a reasonable and appropriate level through the risk management process.

Several resources are available to assist healthcare organizations with the risk analysis process. HHS provides guidance and tools that include a series of papers designed to provide insight into the Security Rule requirements, guidance on specific risks such as remote use, mobile devices, and ransomware, and a link to the Security Risk Assessment (SRA) Tool. This tool provides healthcare providers with a step-by-step guide through the risk analysis process.

If you have questions about cybersecurity or access to the resources available exclusively to SVMIC policyholders, call 800-342-2239 or email ContactSVMIC@svmic.com.

Individuals in your organization such as your administrator, privacy or security officer, or information technology professional may benefit from this article and the other available resources to SVMIC policyholders and staff through their Vantage® account. If someone in

your organization needs a Vantage account, he/she can sign up here.

**If you experience a cybersecurity incident**, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak to the Claims department.

---

*The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.*