ACUVANCE | Coker®

DOWNLOAD

SCAN

HIPAA Security Risk Analysis

Author: **DeAnn Tucker, MHA, RHIA, CHPS, CCS, Senior Manager**



About the **Author**



DeAnn Tucker, MHA, RHIA, CHPS, CHPC, CCS
Senior Manager
Cell: (270) 925-2442
dtucker@cokergroup.com

DeAnn Tucker is a senior manager and holds credentials from the American Health Information Management Association (AHIMA) in HIPAA Privacy and Security, Coding, and Information Management. She also holds credentials for health care privacy with the Health Care Compliance Association (HCCA).

Ms. Tucker has experience as a Privacy and Security Officer and has more than 30 combined years of experience in health information management and health care privacy and security.

DeAnn performs HIPAA Security Risk Analyses, HIPAA Privacy and Security gap assessments, mock desk audits and has served as a virtual privacy officer. She has also provided support and oversight for clients under Corrective Action Plans with the Office for Civil Rights. Her background in health information management and HIPAA compliance provides her with the experience needed to help clients strengthen their overall HIPAA compliance.

Contents

About the Author 2

HIPAA Security Risk Analysis 4

What Is a HIPAA Security Risk Analysis? 5

The HIPAA Security Risk Analysis Process 7

Identify Threats and Vulnerabilities 8

Who requires a HIPAA Security Risk Analysis? 12

Develop Your Risk Remediation Plan 14

Conclusion 14

HIPAA Security Risk Analysis

Experiencing a breach can have a significant financial and reputational impact on healthcare facilities. Although all breaches are not preventable, a facility's best first step is to take a deep dive into its security posture by performing a Security Risk Analysis and identifying where they are vulnerable before cybercriminals exploit such vulnerabilities.

If you experience a significant breach followed by an investigation by the Office for Civil Rights (OCR), your risk management process will be scrutinized. Often, Civil Monetary Penalties result from a lack of due diligence and a failure to accurately and thoroughly assess potential risks and vulnerabilities within your organization.

There is no one way to perform a security risk analysis (SRA). However, this paper will provide tips and options to navigate the process successfully.

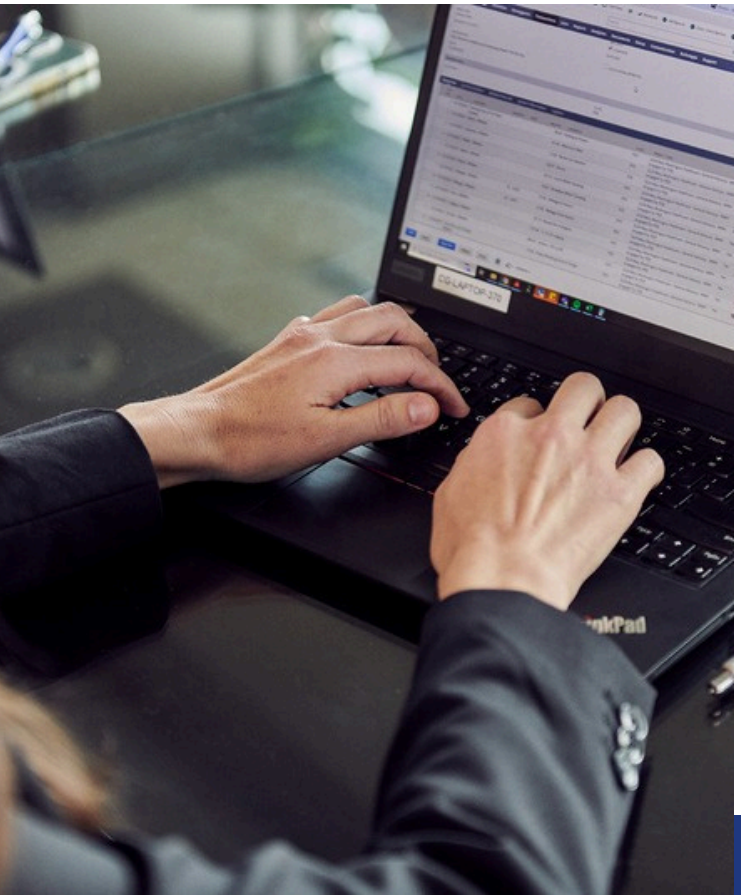
This paper will provide background information on the Department of Health and Human Services requirements to complete a security risk analysis (SRA), explain why you should conduct an SRA, describe key elements of the analysis and explain the importance of creating a follow-up corrective action plan and tracking process.

What Is a HIPAA Security Risk Analysis?

A risk analysis is an accurate and thorough assessment of the potential risks and vulnerabilities to a covered entity's confidentiality, integrity, and availability of electronic protected health information. (45 C.F.R. § 164.308(a)(1)

In a recent corrective action plan announcement, OCR director, Lisa J. Pino, said, "Effective cybersecurity starts with an accurate and thorough risk analysis and implementing all of the Security Rule requirements."

It is the best first step to strengthening your security program.



Key Facts

- SRAs are legally required for healthcare providers to submit electronic claims
- There is no "one way" to perform an SRA
- Start with an inventory of all assets that hold electronic protected health information (ePHI)
- An SRA must identify threats and vulnerabilities to ePHI
- Following an SRA, create a plan to address identified risks
- Don't wait until after you experience a breach to perform an SRA

High-Level SRA Tasks

- Identify assets that hold ePHI
- Identify business associates/ sub-business associates
- Identify threats
- Identify vulnerabilities
- Interview management and other key staff
- Review documented policies and procedures
- Conduct a physical walkthrough
- Identify risks
- Analyze and prioritize risks
- Develop a remediation plan
- Formally document findings & ongoing efforts to improve security posture

How Often?

The requirement to complete an SRA can be found in the HIPAA regulations and is required by the Centers for Medicare and Medicaid Services (CMS). **Neither HIPAA nor CMS specifies how often to conduct an SRA**. HIPAA states that covered entities (CEs) should periodically reassess, while CMS requires a review during each reporting period. Both expect CEs to complete an initial assessment as a baseline, create a mitigation plan from the findings, and implement a continuous monitoring process to correct patient information risks. HIPAA and CMS also expect new or upgraded technology to be added to your risk assessment process. Because these requirements leave room for interpretation, many CEs choose to implement a process for reviewing and revising their SRA yearly. Typically, the first SRA is the most arduous, and implementing a continuous process for evaluating risks can streamline the process and reduce the burden.



The HIPAA Security Risk Analysis Process

Asset Inventory

The best starting point for any organization is to find where the ePHI lives and create an asset inventory. OCR's guidance states the "organization must identify where the ePHI is stored, received, maintained or transmitted." Your asset inventory should include (but is not limited to) applications, laptops, desktops, external memory devices, multi-function machines with hard drives, and medical devices.

Examples Include

- Electronic Medical Record (EMR)
- Medical devices
- Multi-function machines/copiers
- Workstations (laptops/desktops)
- Databases
- Clinical systems (radiology, laboratory, cardiology)
- Other non-clinical systems (email, file share, decision support)
- Cloud Applications



Additional Key Tasks



Create a Business Associate Inventory

- Vendor Name
- Service Provided
- Information Shared
- Contact information



Interview Key Stakeholders

- Information Technology
- Health Information Management
- Compliance Officer



Documentation Review

- Policies
- Procedures
- Training material



Physical Walkthrough

- Information Technology/ Server room and network closets
- Clinical Areas
- Off-site locations

Identify Threats and Vulnerabilities



Risk factors include threats and vulnerabilities. The National Institute of Standards and Technology defines a threat as the potential for a person or thing to exercise a specific vulnerability.

Threats can be:

- Human (intentional and unintentional)
- Nature (flood)
- System failure

A vulnerability is a flaw or weakness in your security program.

Vulnerabilities include:

- Outdated/unsupported operating systems
- The lack of virus protection
- Encryption not implemented where appropriate
- A sprinkler head in the server room
- Overly trusting employee/access management

Assess Risks

Once threats and vulnerabilities have been identified, the next step is to assess the likelihood and potential impact if exploited. The overall risk score considers the effectiveness of existing controls in mitigating threats and vulnerabilities.



The potential impact of a security incident can be broken down into three (3) categories:

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

Potential Impact

- Magnitude of the Loss
- Loss of Revenue & Cost of Repair
- Legal implications
- Impact to Mission
- Loss of public confidence/credibility

Likelihood

- How motivated and capable is threat-source
- How prepared is the organization for this risk area
- Consider existing controls in place
- Ability to detect and respond to the adverse event before it occurs

Likelihood and Impact Scoring Scale Example

IMPACT	LIKELIHOOD
Severe Multi-day interruption, major exposure	**Almost Certain**
Major One day interruption	**Likely**
Moderate Multi-hour interruption, minor exposure	**Moderate**
Minor Multi-minute interruption, no exposure	**Unlikely** Not expected but possible
Insignificant No interruption, no exposure	**Rare** Not expected to occur

Each risk's impact and likelihood scores are combined (i.e., added or multiplied) for a total score that will determine the risk's relevance for further action. A risk assessment chart can be developed to demonstrate where the identified risks rank based on the likelihood and impact analysis. We provide a basic example of a risk assessment chart on the following page.

Risk Assessment Chart Example

#	THREAT	PROBABILITY W/ EXISTING CONTROLS	IMPACT W/ EXISTING CONTROLS	RISK RATING
1	Flood	Low	High	Medium
2	Stolen Laptop	Medium	High	High
3	Unauthorized Access	Medium	High	High
4	Insecure email	Low	Medium	Low

Higher-risk items are prioritized for follow-up and placed on a remediation work plan.



Who requires a HIPAA Security Risk Analysis?

The Health Insurance Portability and Accountability Act (HIPAA) Rules require CEs and business associates (BAs) to safeguard ePHI through reasonable and appropriate security measures. One of these measures required by the Security Rule is a risk analysis, which directs CEs and BAs to conduct a thorough and accurate assessment of the risks and vulnerabilities to ePHI (45 CFR § 164.308(a)(1)(ii)(A)). [1]

Additionally, CMS requires participating providers to conduct or review an SRA annually.

Centers for Medicare and Medicaid Services

Health and Human Services (HHS) is not the only regulatory entity requiring CEs to complete an SRA. CMS requires participating providers to conduct or review an SRA to meet the HIPAA risk analysis standard as part of the Medicare Promoting Interoperability Program attestation process.

The requirement has been part of the interoperability program from the beginning. Its goals are to incentivize the use of technology and encourage clinicians to focus on areas that improve quality and reduce cost.

Non-compliance, submitting inaccurate or incomplete data, or failure to meet the MIPS requirements and score at least 75 points will result in a 9% reduction in reimbursement or payback of previous incentive payments. In 2021, the requirement was 60 points. In each of the past five years, the required score has increased.

Because the threshold is becoming more and more challenging to meet, providers must focus on meeting as many requirements as possible. Completing an SRA should be one of the first requirements to focus on.

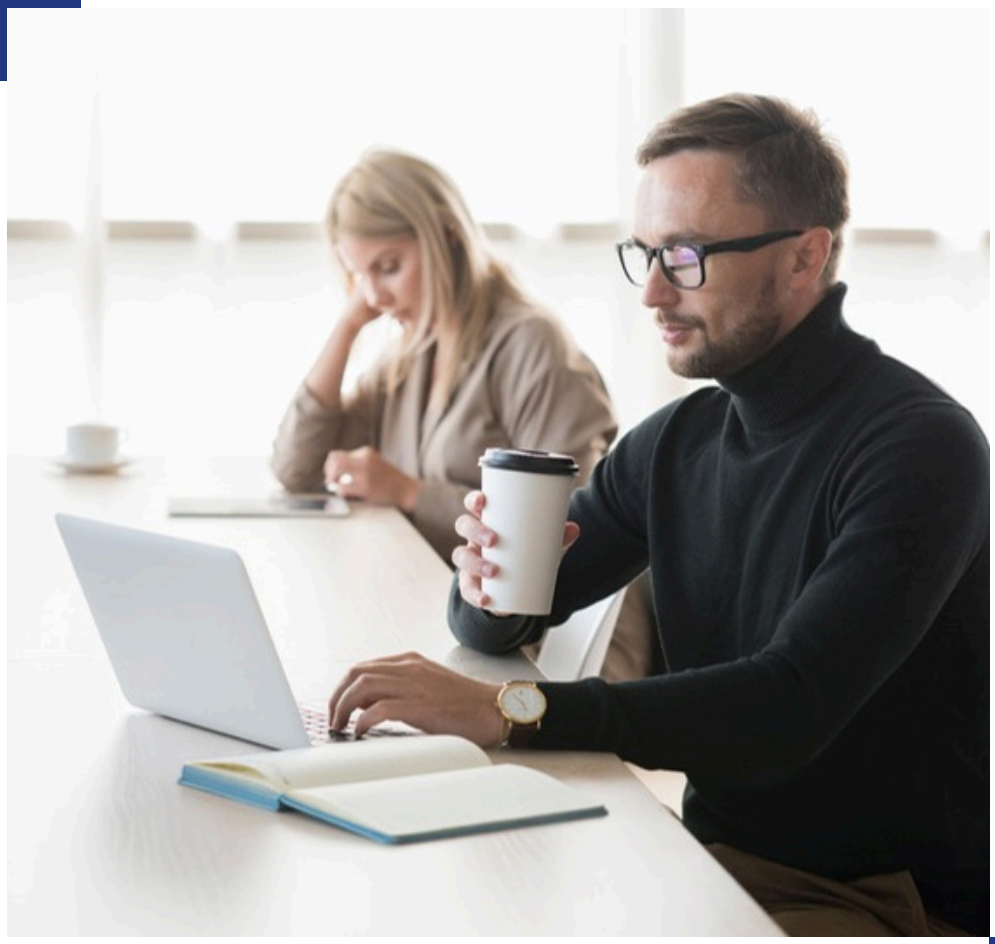
Objective:	**Protect Patient Health Information**
Measure:	**Security Risk Analysis** Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a) (1), including addressing the security (to include encryption) of ePHI data created or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.
Measure ID:	**PI_PPHI_1**

[1] The Office for Civil Rights, Guidance on Risk Analysis Requirements under the HIPAA Security Rule, July 14, 2010.

The CMS includes these additional points of clarification:



- An analysis must be done upon installation or upgrade to a new system, and a review must be conducted covering each MIPS performance period.
- The security risk analysis requirement under 45 CFR 164.308(a)(1) must assess the potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI that an organization creates, receives, maintains, or transmits. This includes ePHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media.
- At a minimum, MIPS-eligible clinicians should be able to show a plan for correcting or mitigating deficiencies and that steps are being taken to implement that plan.[2] Keep in mind that CMS could request proof of an SRA going back six years.



[2] Medicare promoting Interoperability Program Security Risk Analysis ... (n.d.). Retrieved October 6, 2022, from https://www.cms.gov/files/document/sra-safer-guides-information-blocking-fact-sheet422022.pdf

Develop Your Risk Remediation Plan

Risks are ongoing and evolve continuously. As such, your risk management process should be continuous. Eliminating all risks is typically impractical or impossible. Risk remediation should be flexible. A risk management committee should be created to review and approve the risk management plan.

Risk remediation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls.

The security rule specifically states that covered entities should implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. (45 C.F.R. § 164.308(a)(1)(ii)(B)[3]

The following approach is recommended by the National Institute of Standards and Technology (NIST) in its Risk Management Framework.[3]

Prepare
Organization-wide risk assessment

Categorize
Based on risk impact

Select
Determine control needed

Implement

Assess
Are controls working correctly

Authorize
Senior leadership to accept control

Monitor
Continuously monitor

Conclusion

Cyber risks are ever-changing. Healthcare organizations should continuously evaluate their environment. An accurate and thorough security risk analysis is one of the most important tasks a covered entity can complete.

A thorough SRA could help you prevent major security incidents as well as potentially reduce civil monetary penalties assessed as a result of a major breach. Most importantly, an SRA will help you protect your patients' information.

If you have not completed your SRA, contact us today. We will help you identify your risk and vulnerabilities, review your documentation, perform a vulnerability scan and help you create a remediation plan.

[3] Computer Security Division, I. T. L. (n.d.). NIST Risk Management Framework: CSRC. CSRC. Retrieved October 5, 2022, from https://csrc.nist.gov/Projects/Risk-Management



ACUVANCE | Coker®

For further information, please contact:

(800) 345-5829
askcoker@cokergroup.com
visit cokergroup.com