Rural Focus

December 2020

How Important Is a HIPAA Security Risk Analysis?

By DeAnn Tucker, M.H.A., RHIA, CHPS, CCS, Senior Manager, Coker Group

It is well known that experiencing a breach can have a significant financial and reputational impact on healthcare facilities. Rural hospitals specifically are very familiar with financial struggles. According to UNC's Cecil G. Sheps Center for Health Services Research, 134 rural hospitals have closed since 2010.[1] Often, these rural facilities provide the primary point of access to healthcare and are typically the area's largest employer. Not all breaches are preventable, but the *best first step* a facility can take is to take a deep dive into their security posture and self-identify where they are vulnerable before that vulnerability is exploited. If you experience a significant breach and a follow up investigation by the Office for Civil Rights, consideration will be given to your risk management process. Often times we see Civil Monetary Penalties result from a lack of due diligence and a failure to conduct an accurate and thorough assessment of potential risks and vulnerabilities.

The Office for Civil Rights (OCR), which is responsible for enforcing the Privacy and Security Rules, issued guidance that provides Covered Entities (CEs) and Business Associates (BAs) assistance in compliance with the risk analysis requirement. In the guidance, OCR explains that "conducting a risk analysis is the first step in identifying and implementing safeguards" and further clarifies "all e-PHI is subject to the Security Rule." The requirement to perform a Security Risk Analysis (SRA) is in §164.308(a)(1)(ii)(A), "RISK ANALYSIS (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [covered entity]." The guidance further states that the SRA process should be "ongoing," and they recognize that the frequency will vary among CEs. Additionally, they advise CEs to perform an SRA on new technology and when business operations change.[2]

Key Board Takeaways

- There is no "one way" to perform an SRA.
- An SRA must identify threats and vulnerabilities to your ePHI.
- Create a plan to address identified risks.
- Don't wait until after you experience a breach.
- Conducting or reviewing an SRA is required for participants of the Medicare and Medicaid EHR Incentive Programs as well as HIPAA.

However, Health and Human Services (HHS) is not the only regulatory entity requiring CEs to complete an SRA. The Centers for Medicare and Medicaid Services (CMS) require participating providers to conduct or review an SRA to meet the HIPAA risk analysis standard as part of the Medicare and Medicaid EHR Incentive Programs attestation process. The incentive programs have seen many changes over the last several years, and it has always included the requirement to do an SRA. Just as the HIPAA requirement was not specific in their requirement, neither was the CMS guidance. However, we do find this clarification:

It is acceptable for the security risk analysis to be conducted or reviewed outside the performance period; however, the analysis must be unique for each performance period,

1 See www.shepscenter.unc.edu/programs-projects/rural-health/rural-hospital-closures/.
2 The Office for Civil Rights, Guidance on Risk Analysis Requirements under the HIPAA Security Rule, July 14, 2010.

the scope must include the full MIPS performance period, and it must be conducted within the calendar year of the MIPS performance period (January 1–December 31)...and a review must be conducted covering each MIPS performance period. Any security updates and deficiencies that are identified should be included in the clinician's risk management process and implemented or corrected as dictated by that process.[3]

The annual SRA requirement does not state that an entirely new SRA is required, but at a minimum, CEs are required to review and update the SRA annually.

3 The Centers for Medicare and Medicaid Services, Merit-Based Incentive Payment System (MIPS) Promoting Interoperability Performance Category Measure 2020 Performance Period.

Exhibit 1: MIPS Promoting Interoperability Performance Category Measure, 2020 Performance Period

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**

Note: In order to earn a score greater than zero for the Promoting Interoperability Performance Category, MIPS eligible clinicians must submit a "yes" that they have completed the Security Risk Analysis measure during the calendar year *in which the MIPS performance period occurs.*

Source: The Centers for Medicare and Medicaid Services.

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. Any security updates and deficiencies that are identified should be included in the clinician's risk management process and implemented or corrected as dictated by that process.
- 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.[4]

We can find guidance in two other primary places: the preamble and corrective action plans published on the HHS Web site.[5] In the preamble, we find some clarification as to how

4 *Ibid.*
5 See www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html.

often you should conduct an SRA stating security measures "must periodically be reassessed and updated as needed." It provides further explanation stating, "the risk analysis must look at risks to the covered entity's electronic protected health information. A thorough and accurate risk analysis would consider 'all relevant losses' that would be expected if security measures were not in place."[6]

Over the last few years, many Corrective Action Plans (CAPs) have mentioned non-compliance with the requirement to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI."[7] In particular, one CAP provides some beneficial information. On July 22, 2019, HHS published the *Notice of Proposed Determination for Jackson Health* System (JHS) and later published the *Notice of Final Determination* informing the health system that the $2,154,000.00 civil money penalty was final.[8] OCR points out the following details related explicitly to the SRA requirement:

- The 2017 SRA erroneously identified several provisions of the Security Rule as "not applicable."
- The 2014 SRA failed to include all ePHI and did not identify the totality of threats and vulnerabilities.
- JHS did not remediate risks, threats, and vulnerabilities identified in 2014 by implementing recommendations provided by a third party.
- The 2015 SRA did not include all ePHI and did not identify the totality of threats and vulnerabilities, and some sections were left blank.
- JHS did not remediate risks, threats, and vulnerabilities identified in 2015, and the same high risks identified in 2014 were still identified as high risks.
- The 2016 SRA identified the same high risks as 2014 and 2015 with no remediation.
- The 2017 SRA was compartmentalized and not thorough in scope. In addition, the methodology used was primarily limited to policy review and interviews.
- JHS continually failed to conduct a sufficient, enterprise-wide risk analysis that meets the requirements of 45 CFR 164.308(a)(1)(ii)(A).[9]

Additionally, the corrective action plan states that the basis of the Civil Monetary Penalties were in part due to Jackson Health System's failure to implement policies and procedures to prevent, detect, contain, and correct security violations because it failed to conduct an accurate and thorough assessment of potential risks and vulnerabilities. It is also pointed out that for many years, there was no evidence that Jackson Health System remediated any of its risk to ePHI. That failure contributed to the overall $2,154,000.00 penalty.

How Often Should an Assessment Be Conducted?

Neither HIPAA nor CMS specifically require a yearly SRA. HIPAA states 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 chose 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.

High-Level Checklist

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

Where to Start?

If you have not completed your initial SRA, start today. There are many helpful resources available on the Health and Human Services Web site, and consulting companies are available to help you. A great starting point for any organization is to find where your ePHI lives and create an asset inventory.

6 Department of Health & Human Services, Centers for Medicare & Medicaid Services, Health Insurance Reform: Security Standards, Federal Register, Vol. 68, No. 34, February 20, 2003.
7 Timothy Noonan to Judy Ringholz, RN, J.D., CHC, Jackson Health System Notice of Proposed Determination, July 22, 2019, Department of Health & Human Services.
8 Roger Severino to Judy Ringholz, RN, J.D., CHC, Jackson Health System Notice of Final Determination, October 15, 2019, Department of Health & Human Services.
9 Noonan, 2019.

The "organization must identify where the ePHI is stored, received, maintained or transmitted."[10] 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.

After finding all of your ePHI, start identifying your risks. 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 (hacker) or nature (flood). A vulnerability is a flaw or weakness in your security program. Vulnerabilities can be using an operating system that is no longer supported and receiving updates, the lack of virus protection or encryption, a sprinkler head in your server room, or an error in the set-up of access to ePHI. Identifying your risks before someone identifies them can help you prevent a breach.

HealthIT.gov has created and published a free tool to help small organizations. However, there is a disclaimer directly on their Web site that this tool is provided for informational purposes only and does not guarantee compliance. Still, it can give you some insight as to what an SRA should look like.

10 The Office for Civil Rights, 2010.

The Governance Institute thanks DeAnn Tucker, M.H.A., RHIA, CHPS, CCS, Senior Manager, Coker Group for contributing this article. She can be reached at dtucker@cokergroup.com.