Comagine Health

Quality Payment Program

Small, Underserved and Rural Support

Security Risk Analysis

The Security Risk Analysis (SRA) is a requirement for the Promoting Interoperability (PI) category of the Merit-based Incentive Payment System (MIPS) as well as the HIPAA Security Rule, which requires covered entities including health plans, most health care providers (including doctors, clinics, hospitals, nursing homes and pharmacies), health care clearinghouses and their business associates to conduct a risk assessment of their health care organization on a regular basis. Although no points are associated with this measure for PI, failure to attest to this requirement when submitting data for MIPS will result in a score of zero for the PI category.

The purpose of the SRA is to find any potential risks to the security of your organization's protected health information (PHI). The SRA is required at the following times, and ongoing monitoring is also required:

- An SRA must be completed or reviewed at least annually (whether reporting for MIPS or not).
- An SRA should be conducted with any major change, such as significant changes in infrastructure, technology or staffing.
- An SRA is required upon installation or upgrade of an electronic health record (EHR), such as when you upgrade from 2014 to 2015 Edition certified electronic health record technology (CEHRT).

Note that for MIPS, the SRA may be conducted or reviewed outside the PI performance period; however, the analysis must be unique for each performance period, the scope must include the full MIPS performance period, and it must be conducted within the calendar year of the MIPS performance period (Jan. 1 – Dec. 31).

What the SRA Covers

The SRA helps an organization comply with HIPAA's administrative, physical and technical safeguards.

- Administrative safeguards are administrative functions that should be implemented to meet the security standards, such as assignment or delegation of security responsibility to an individual, as well as security training for all staff.
- Physical safeguards are mechanisms required to protect electronic systems, equipment and the data they hold from threats, environmental hazards and unauthorized intrusion. This includes building security, locked server rooms, visitor restrictions, etc. Physical safeguards also include restricting access to electronic protected health information (ePHI) and retaining off-site computer backups.
- Technical safeguards are primarily the automated processes used to protect data and control access to data, such as using authentication controls to verify that the person signing onto a computer is authorized to access that ePHI, or encrypting and decrypting data as it is being stored and/or transmitted. Other technical safeguards include using secure passwords, locking workstations when away and not sharing passwords.

Resources for SRA Completion

The Security Rule Guidance Material from CMS provides the SRA Tool, sample business associate agreements, an explanation of HIPAA policies and many other items. Reviewing this is a good place to start, as you have several choices for how to complete your SRA.

Your practice may complete it yourselves using a downloadable Security Risk Assessment Tool (SRA Tool Version 3.0.1), which was developed by the Office of the National Coordinator for Health Information Technology (ONC) in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), or a similar tool. This is a downloadable computer program that offers guidance to the operator as the SRA is being completed. A downloadable SRA Tool 3.0.1 User Guide (PDF) is available to guide you as well.

The SRA Tool (version 2.0) also has a paper version, which is downloadable in three sections:

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards

Completion of your SRA internally will take some time, so plan accordingly. Larger practices may have an IT department to complete the SRA, but do not assume it is being done. Secure a copy of the completed SRA for your records. If you do not have the internal resources to complete the SRA, you may contract with an outside agency to do it.

Note that your EHR vendor generally is not completing your practice's SRA. They do not have all of the information to do this unless it is a contracted service they offer. They would then need to come to your office or have some other means of working directly with the practice to complete the tool. If you believe your EHR vendor has completed this on your behalf within the year, request a copy for your records and verify that what they provide is a full SRA as required by CMS.

Getting Started with Security Risk Analysis

Before you start your SRA, check whether your practice has completed an SRA in the past. If so, collect the following information on the previous SRA:

- Date completed
- Method of completion (downloadable tool, IT department, outside agency)
- Risks identified and corrective action plan developed

You should also check whether you have recently upgraded your EHR or purchased a new system. If so, determine the date of the upgrade or purchase and find whether the SRA was completed or reviewed after this upgrade.

Once you have determined that you need to complete a new SRA for this year and know when you will work on it, consider the following steps to work through the process:

1. Identify who will complete the SRA for your practice. If attempting to identify an outside agency to assist you, contact your professional organizations for recommendations and reviews on third-party agencies.
2. If you plan to complete the SRA internally, decide whether you will use the ONC SRA Tool or a similar tool. The following resources may be useful:
   - View the SRA videos available from HealthIT.gov for guidance on the process.
   - Print the Security Risk Assessment (SRA) Tool 2.0 User Guide (PDF) or the SRA Tool 3.0.1 User Guide (PDF).
3. If using the ONC SRA Tool, download the SRA Tool. The link is found in the yellow box on the webpage. It is a self-contained tool that can be run on a Windows desktop or laptop computer. You will need to have access and authorization to download and run programs on your computer to be able to install and run the program. You may need to work with your IT department to accomplish this. Consider if you will need to have mobile access to the SRA Tool when using the downloaded program. If so, installation on a laptop or Windows-based tablet may be advisable.

If you want to use the previous iPad version, search the Apple App Store for "HHS SRA Tool". A paper-based version of the tool is also available on the webpage.

4. Plan sufficient time to complete the SRA as it is a lengthy process. Set aside time on a regular basis for this work and consider that it may take multiple people to complete.

Resources

- **2019 Security Risk Assessment Tool Administrative Safeguards.** (2019). CMS. https://www.healthit.gov/sites/default/files/attachment_b_-_20140312_sratool_content_-_administrative_volume_v6_clean.docx
- **2019 Security Risk Assessment Tool Main Page.** (2019). CMS. https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- **2019 Security Risk Assessment Tool User Guide.** (2019). CMS. https://www.healthit.gov/sites/default/files/page/2019-03/SRAT_v3.0.1_User_Guide.pdf
- **Perform a Security Risk Analysis: Top FAQs and Tips for Success.** (2015). American Academy of Ophthalmology. https://www.aao.org/eyenet/article/perform-security-risk-analysis-top-faqs-tips-succe?april-2015
- **Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices.** (2018). HealthIT.gov. https://www.healthit.gov/resource/reassessing-your-security-practices-health-it-environment-guide-small-health-care
- **Security Risk Analysis 2019 Measure Specification Document**. (2019). CMS. https://tmfnetworks.org/Portals/0/Documents/QPP/2019MIPSPIMeasuresSecurityRiskAnalysis.pdf
- **Security Risk Assessment Videos.** (2017). HealthIT.gov. https://www.healthit.gov/topic/privacy-security/security-risk-assessment-videos
- **Security Rule Guidance Material.** (2019). CMS. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- **The Security Rule.** (2019). CMS. https://www.hhs.gov/hipaa/for-professionals/security/index.html
- **Top 10 Myths of Security Risk Analysis.** (2017). HealthIT.gov. https://www.healthit.gov/topic/privacy-security/top-10-myths-security-risk-analysis

This material provided by Comagine Health, the Medicare Quality Innovation Network - Improvement Organization, was prepared by TMF Health Quality Institute, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents presented do not necessarily reflect CMS policy. 12SOW-GEN-20-QIN-038