HIPAA Security Risk Assessment Tool

The Department of Health and Human Services (HHS), through its Office of the National Coordinator for Health Information Technology (ONC), developed an interactive **Security Risk Assessment Tool (SRA Tool)** to assist covered entities in performing and documenting Health Insurance Portability and Accountability Act (HIPAA) security risk assessments.

Although HHS designed the SRA Tool for health care providers in small- to medium-sized offices, it is a helpful resource for all covered entities and business associates to review their implementation of the HIPAA Security Rule. HHS updated the SRA Tool in September 2023 to incorporate a variety of new enhancements and bug fixes based on user feedback from prior versions.

Conducting a risk assessment is a **crucial first step** in an organization's efforts to comply with the Security Rule. It directs what reasonable steps a covered entity or business associate should take to protect the ePHI it creates, transmits, receives or maintains. Risk assessment is also an **ongoing process**. Covered entities and business associates should periodically revisit their risk assessments and make appropriate updates to their ePHI safeguards.

LINKS AND RESOURCES

- Access the SRA Tool here
- SRA Tool User Guide
- SRA User Videos

HIGHLIGHTS

RISK ASSESSMENT

- Covered entities and business associates must analyze the potential risks and vulnerabilities of their ePHI.
- Based on this analysis, covered entities and business associates must implement reasonable and appropriate safeguards.
- Risk assessment is an ongoing process.

SRA TOOL

- The SRA Tool can help guide a covered entity through the risk assessment process.
- It is a Windows-based application (or Excel workbothat can be run on a user's computer.
- The tool merely collects data; it does not send data anywhere else.

WHY IS A RISK ASSESSMENT IMPORTANT?

The HIPAA Security Rule requires covered entities (including group health plans) and business associates to conduct an accurate and thorough analysis of the potential risks and vulnerabilities of the **confidentiality, integrity and availability** of their electronic protected health information (ePHI). Covered entities and business associates must then implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of ePHI.

Conducting a risk assessment is a **crucial first step** in an organization's efforts to comply with the Security Rule. It directs what reasonable steps a covered entity or business associate should take to protect the ePHI it creates, transmits, receives or maintains.

A risk assessment helps an organization establish appropriate administrative, physical and technical safeguards for its ePHI.

Risk assessment is also an **ongoing process**. Covered entities and business associates should periodically revisit their risk assessments and make appropriate updates to their ePHI safeguards. According to HHS, compliance with the HIPAA Security Rule is not a one-time project, but rather an ongoing, dynamic process that will create new security challenges as organizations and technologies change.

HHS' Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Security Rule. OCR has increased its enforcement of the HIPAA Privacy and Security Rules in recent years, with some costly outcomes for covered entities. Failing to conduct a timely and thorough risk assessment has routinely been identified by OCR as a **common HIPAA compliance problem**. Given this increased enforcement activity, an accurate and thorough risk assessment is more important than ever for covered entities and business associates.

WHAT SECURITY SAFEGUARDS ARE REQUIRED?

The HIPAA Security Rule does not require covered entities and businesses associates to follow a specific risk assessment methodology. As the health care industry is both diverse and broad, the HIPAA Security Rule is designed to be flexible and scalable. The Security Rule recognizes that the methods used by a covered entity or business associate to safeguard ePHI will vary based on the size, complexity and capabilities of the organization.

As part of the ongoing risk assessment process, organizations should assess and document the security measures used to safeguard ePHI, evaluate whether the security measures required by the Security Rule are in place and determine whether current security measures are configured and used properly.

If an organization determines that its security measures are not sufficient to protect against evolving threats or vulnerabilities, a changing business environment or the introduction of new technology, the organization must determine whether additional security measures are needed.

HOW DOES THE SRA TOOL WORK?

The SRA Tool is a downloadable tool that can be used by a covered entity or business associate as a resource (among other tools and processes) to review its implementation of the HIPAA Security Rule.

The SRA Tool has two versions: a Windows-based application that can be downloaded and run on a user's computer and an Excel workbook that takes the same content from the Windows application and presents it in a spreadsheet format. To download the SRA Tool, visit ONC's website at www.healthit.gov/security-risk-assessment.

The SRA tool contains questions that address administrative, technical and physical safeguards—including basic security practices, security failures, risk management and personnel issues. Each question includes resources to help users:

- Understand the context of the question;
- Consider the potential impacts to ePHI if the requirement is not met; and
- See the actual safeguard language of the HIPAA Security Rule.

Users of the SRA Tool can document their answers, comments and risk remediation plans directly into the Tool. The SRA Tool can support an organization's risk assessment process. Responses to the questions in the SRA Tool can be used to help organizations identify areas where security controls designed to protect ePHI may need to be implemented or where existing implementations may need to be improved.

The SRA Tool's webpage contains a User Guide and tutorial video to help organizations begin using the tool. Videos on risk analysis and contingency planning are available on the ONC website to provide further context.

KEEP THESE IMPORTANT POINTS IN MIND:

- Completing a risk assessment requires a **time investment**.
- The SRA Tool is self-contained. Input is stored in the user's computer for future reference and generating reports, but the **data is not sent anywhere else** (for example, the data is not sent to HHS).
- The SRA Tool was developed with small- to medium-sized health care providers in mind. Some of the questions may not be applicable to health plans, or may need to be adapted to fit the health plan context.
- The SRA Tool **does not guarantee HIPAA compliance**. According to HHS, organizations may use the SRA Tool in coordination with other tools and processes to support their risk analysis and risk management activities. Also, the SRA Tool does not address requirements of the HIPAA Privacy Rule.