Brought to you by Cottingham & Butler

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), has 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.

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**, and will likely be a focus of future OCR compliance audits. 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. The HIPAA Security Rule requires covered entities and business associates to implement **administrative, physical and technical security measures**.

Administrative Safeguards	Physical Safeguards	Technical Safeguards
Establish standards and specifications for your health information security program Examples: • Security management processes to identify and analyze risks to ePHI • Implementation of security measures to reduce risks • Staff training to ensure knowledge of and compliance with policies and procedures • Information access management to limit access to ePHI • Contingency plan to respond to emergencies or restore lost data	Control physical access to your office and computer systems Examples: • Facility access controls, such as locks and alarms, to ensure only authorized personnel have access to facilities that house systems and data • Workstation security measures, such as cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users • Workstation use policies to ensure proper access to and use of workstations	Include hardware, software and other technology that limits access to ePHI Examples: • Access controls to restrict access to ePHI to authorized personnel only • Audit controls to monitor activity on systems containing ePHI • Integrity controls to prevent improper ePHI alteration or destruction • Transmission security measures to protect ePHI when transmitted over an electronic network

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 software application 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 can be downloaded free of charge and run on a user's desktop or laptop computer. To download the SRA Tool, visit ONC's website at www.healthit.gov/security-risk-assessment.

An iPad® version of the SRA Tool is also available at no cost and can be downloaded from Apple's App Store.

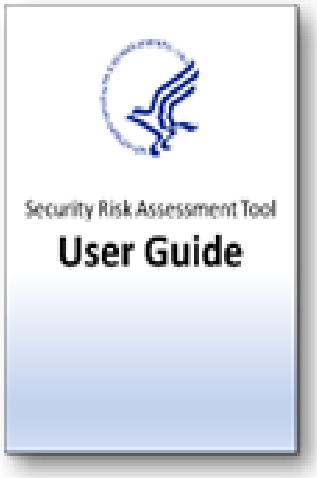
The tool's content is also available in three Microsoft Word® documents that can be downloaded or printed from the ONC website.

HIPAA Security Risk Assessment Tool

The SRA tool contains **156 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 Web page 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.

ONC is asking for users' feedback, which may be used to improve future versions of the tool.

KEEP THESE IMPORTANT POINTS IN MIND:

- Completing a risk assessment requires a **time investment**. Users of the SRA Tool may sign in and out multiple times and their information will be saved.
- 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.