The Security Risk Assessment Tool

Overview for Small and Medium Practices

Presenters: Ryan Callahan, Nick Heesters
Agenda

• What is a Security Risk Assessment?
• Overview of the SRA Tool
• Enhancements in Version 3.4
• Q&A
What is Security Risk Assessment?

A **covered entity** or **business associate** must:

“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the organization”

HIPAA § 164.308(a)(1)(ii)(A)
Risk Analysis components of a Security Risk Assessment:

- Identifying all ePHI within your organization.
- Identifying sources of ePHI
- Identifying human, natural, and environmental threats to information systems that contain ePHI.
Outcomes from security risk assessment

Organizations should use information gleaned from their assessment to implement security measures to:
- Design personnel screening processes
- Identify and strategize data backup
- Determine where and how encryption should be used
- Determine what authentication may be required to protect data integrity
- Determine which policies and procedures may need to be created or improved to protect ePHI
Challenge
- Organizations are vulnerable
- SRA is required
- Small budgets, few staff

SRA Tool
An accessible, wizard-based tool to aid in the identification and assessment of risks to ePHI.
The SRA Tool
Downloading, Installing, and Using the SRA Tool
Download & Installation

The tool can be downloaded from HealthIT.gov. The downloaded file is the installer for the tool. Double click to run the installer and walk through install process.

Once downloaded, a blue “SRA-Tool” icon will appear on your desktop.

Note: Users must have administrative privileges in order to install the SRA Tool. For this reason, you may need help from your IT department or system administrator to install the tool. Admin privileges are not needed to run the tool once it has been installed.

The tool runs on Windows, 7, 8, 10 and 11. All information entered into the tool is contained locally. No information is transmitted to DHHS, ONC or OCR.
Welcome Screen

Select “Start New SRA” or “Continue SRA” to begin using the tool.

Enter your name, name your SRA file and select a location to save your SRA file locally.

The “Check for Updates” feature allows you to see if new content updates have been released by ONC.
When beginning a new assessment, the user is asked to enter their name.

It is recommended to enter your full first & last name.

The SRA Tool supports multiple user accounts, so more than one person can work on an in progress SRA file.
Saving a New SRA File

The SRA Tool creates SRA files that can only be opened with the SRA Tool application.

After entering your name, you then select a file name and save location for the new .sra file.

Files with the .sra extension can be opened and edited with the SRA Tool application.
Practice Information, Asset & Vendor Management

A place to track:
- Practice locations
- Assets (computers, equipment, other hardware)
- Business Associates (vendors)
- Attached documents
The Assessment section contains 7 sections with multiple-choice questions and branching logic.

The Education panel provides guidance related to each response given.

The Reference panel links each question to a HIPAA Security Rule citation.

Progress indicators are provided in the navigation panel as sections are completed.
Threats & Vulnerabilities

The Vulnerability Selection and Threat Rating section is presented after each section of multiple-choice questions.

Users are asked to select from a list of vulnerabilities that may be applicable to their practice.

Each vulnerability comes with a list of related threats that must be rated for the likelihood they may occur and the impact they would have should they occur.
Each section is concluded with a Section Summary. The Section Summary shows each of the questions answered, responses, and education content.

Questions are divided into **Areas of Success** and **Areas for Review**. Questions sorted into Areas of Success are those which represent the highest level of compliance. Areas for Review represent responses that could use improvement.

Users can enter **Additional Information** specific to each assessment section and add/link relevant documents necessary to demonstrate accuracy and thoroughness of responses.
Reports
Summary Report

After all sections are complete, the Summary section becomes available.

The Summary Report is high level summary of your risk assessment.

Risk Score – shows the number of questions sorted into Areas for Review divided by the total questions the user answered.

Areas for Review – shows the total number of questions answered sorted into Areas for Review.

Vulnerabilities – shows the total number of vulnerabilities selected as applicable to the practice or organization.

Each assessment section's Risk Score is shown as a percentage.
The Risk Report identifies all areas of risk collected across your entire assessment.

Each vulnerability selected is shown here along with each response that fell into the category Areas for Review.

Risk Breakdown – shows a sum of threat ratings in each risk level (Low, Medium, High, and Critical).

Risk Assessment Rating Key – shows how likelihood and impact ratings combined create the risk level.
The Risk Report displays the selected Vulnerabilities and Threat Ratings, as well as, all questions that were sorted into “Areas for Review”.

Users can review the question, their answer, and the education guidance so they know how to improve their security and mitigate risk in that area.
The Detailed Report is a collection of all data captured throughout the entire assessment.

Each question and response, each threat and vulnerability rating, all of the Practice Information, Assets, and Vendor information is shown in the Detailed Report. There is also an audit log of each contributing user with a date/time stamp.

Export a PDF or Excel copy of the report using the Export Options button.
What to Expect

• Invest a significant amount of time.
• The value of the SRA to your organization depends on the integrity of the input.
• Spend time on understanding requirements, security, where ePHI exists within your organization’s IT environment, and what threats to consider.
• Ensure an inclusive scope. This means all IT assets which create, maintain, receive, or transmit ePHI.
• Regarding applications, be sure to look beyond just the EHR system.
  • *For example: Practice management, scheduling, billing, telecommunications, e-mail, cloud apps, and other platforms can all contain or access ePHI*
Enhancements in Version 3.4
Glossary Page – terms and definitions provided in one place for easy access

Embedded Definitions – tooltips embedded in the SRA Tool content to provide more information without leaving the page
Remediation Report

- Additional Report
- Identifies areas of risk
- Place to respond to known risk, outline plan to move forward
- Assign owner
- Assign completion date
- Link documents
- Print
HICP 2023 Edition Updates


- New references added
- Links updated
Content Version Warning

Warns user that the file they are working on is old and new questions may be available.

Must be dismissed each time old file is opened.
Copy text, and others...

- Copy text from Education and References panes for easy reference outside the tool.
- Improve PDF report format
- Pre-populate filename when saving
- Other usability improvements and bug fixes
# Excel Workbook

Released initially with SRA Tool Version 3.3.

Provides an alternative to the software tool for those who cannot run it or those who would prefer to work with the content in spreadsheet format.
Conducting a Thorough Assessment

The HIPAA Security Rule’s risk analysis requires an accurate and thorough assessment of the potential risks and vulnerabilities to all of the ePHI the organization creates, receives, maintains, or transmits.

• When responding to questions to identify and assess potential risks, organizations should consider how the questions apply throughout its entire enterprise.
• Organizations should take care that its responses reflect an accurate and thorough assessment of the questions presented, and are not merely a clerical exercise to produce a report.
• Responding to questions without considering how the questions apply throughout the organization may result in a risk analysis that is not accurate and thorough as required by the HIPAA Security Rule.
Frequently Asked Questions

How do I upgrade to the latest version of the SRA Tool without starting over from scratch?
The installer is designed to overwrite the previous version of the tool without issue. Files created with previous versions of the tool will still work. However, if you continue working on older files, you may be missing out on content updates.

How do I update the Audit Date displayed in the Detailed Report.
Audit Date reflects the last date a question was updated. The Audit Date will only be changed if the response is changed. If you’ve reviewed and updated an older SRA file, the date of review can be included in your file name or Date modified.

Is SRA Tool available for Apple or Mac computers?
No. The desktop application does is not supported on MacOS, Linux, or any operating system other than Windows. If you wish to use the SRA Tool on one of these systems, you might consider the SRA Tool Excel Workbook.

Does the SRA File or report need to be submitted anywhere?
Your SRA is for your own records. It may be required for an incentive program like MIPS, but that is outside of the scope of the tool. SRA files are not submitted to ONC or OCR.
Questions From Chat
Contact Us

Contact the SRA Tool Helpdesk:
Email: SRAHelpDesk@Altarum.org

Submit SRA Tool Questions via the HealthIT Feedback Form
Additional Information & Resources

- Visit HealthIT.gov and the SRA Tool Download page
- SRA Tool User Guide on the SRA Tool Download Page
- Guide to Privacy and Security of Electronic Health Information
- HealthIT Privacy and Security Resources for Providers

Follow @ONC_HealthIT on Twitter for updates on the SRA Tool