The Security Risk Assessment Tool

Overview for Small and Medium Practices

Presenters: Ryan Callahan, Nick Heesters

Altarum

Office of the National Coordinator for Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

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

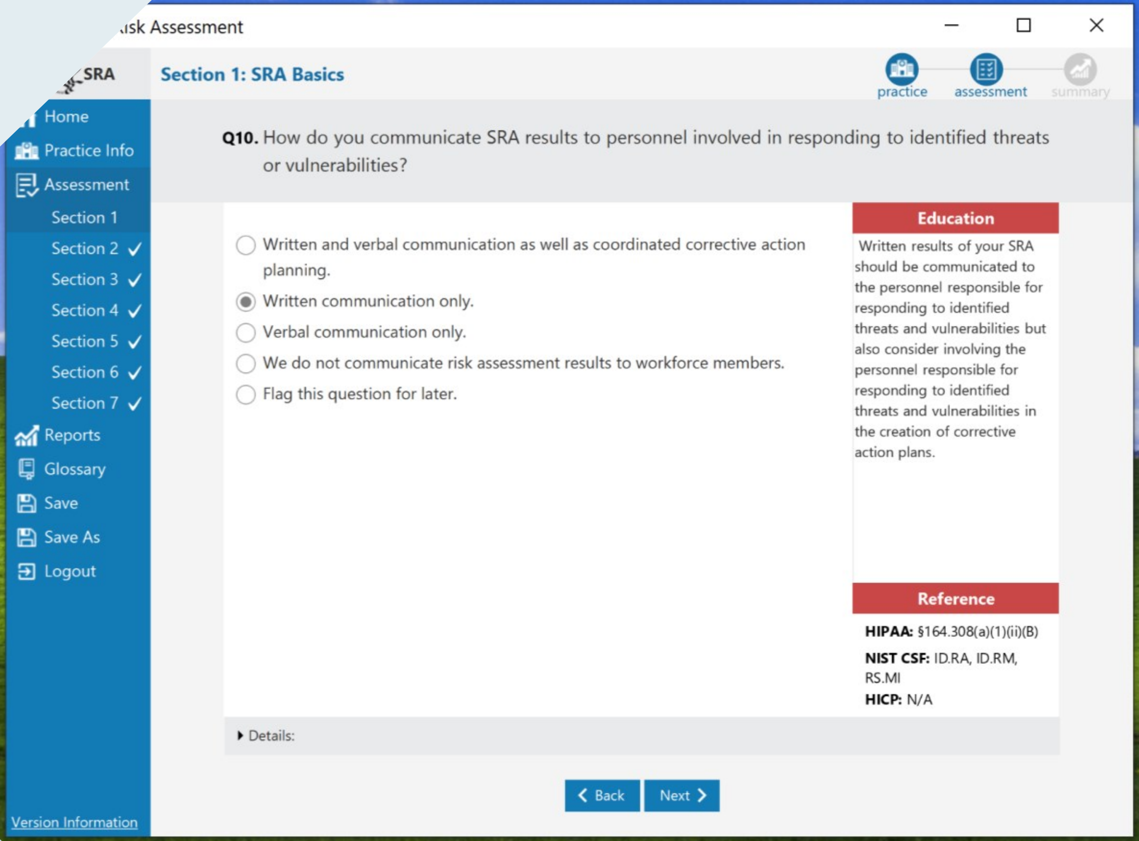
Challenge

- Organizations are vulnerable
- SRA is required
- Small budgets, few staff

SRA Tool

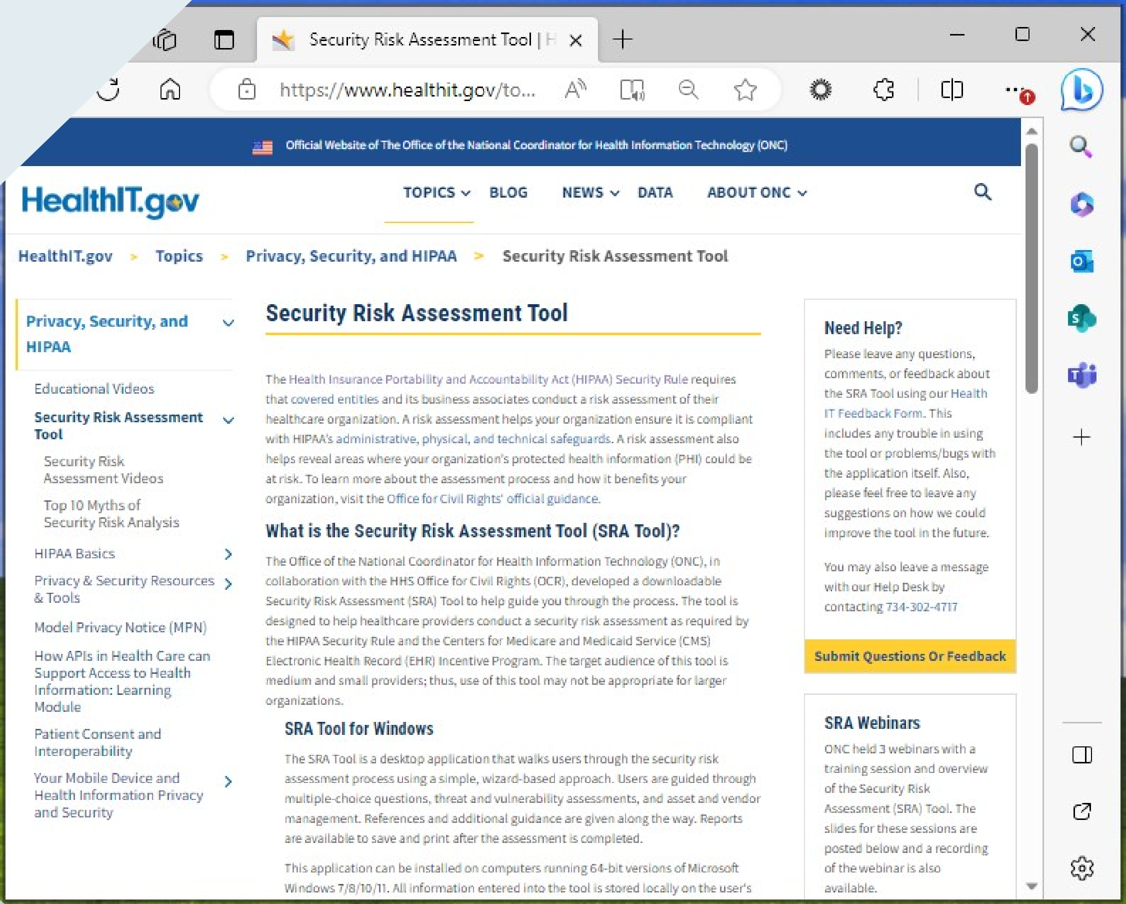
An accessible, wizard-based tool to aid in the identification and assessment of risks to ePHI.

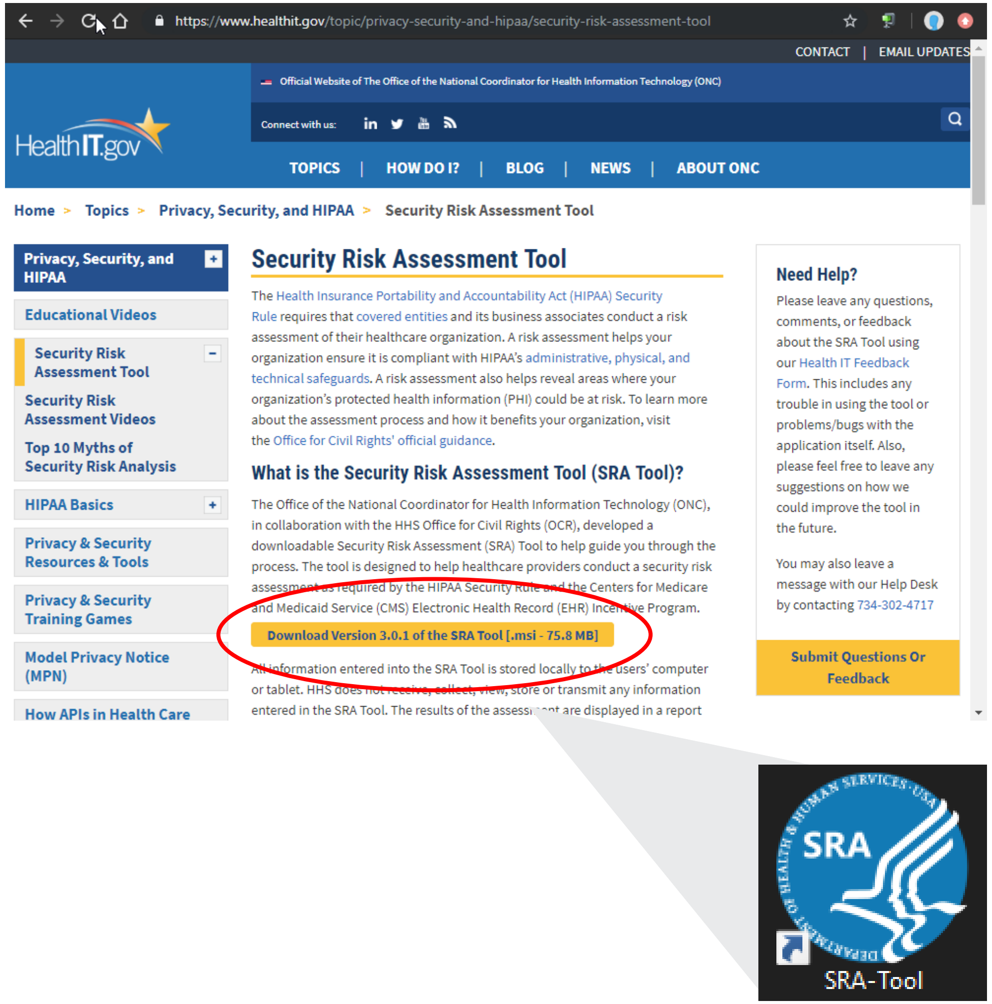
The SRA Tool



isk Assessment
SRA
Section 1: SRA Basics
practice
assessment
summary
Home
Practice Info
Assessment
Section 1
Section 2
Section 3
Section 4
Section 5
Section 6
Section 7
Reports
Glossary
Save
Save As
Logout
Version Information
Q10. How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?
Written and verbal communication as well as coordinated corrective action planning.
Written communication only.
Verbal communication only.
We do not communicate risk assessment results to workforce members.
Flag this question for later.
Education
Written results of your SRA should be communicated to the personnel responsible for responding to identified threats and vulnerabilities but also consider involving the personnel responsible for responding to identified threats and vulnerabilities in the creation of corrective action plans.
Reference
HIPAA: §164.308(a)(1)(ii)(B)
NIST CSF: ID.RA, ID.RM, RS.MI
HICP: N/A
Details:
Back
Next

Downloading, Installing, and Using the SRA Tool





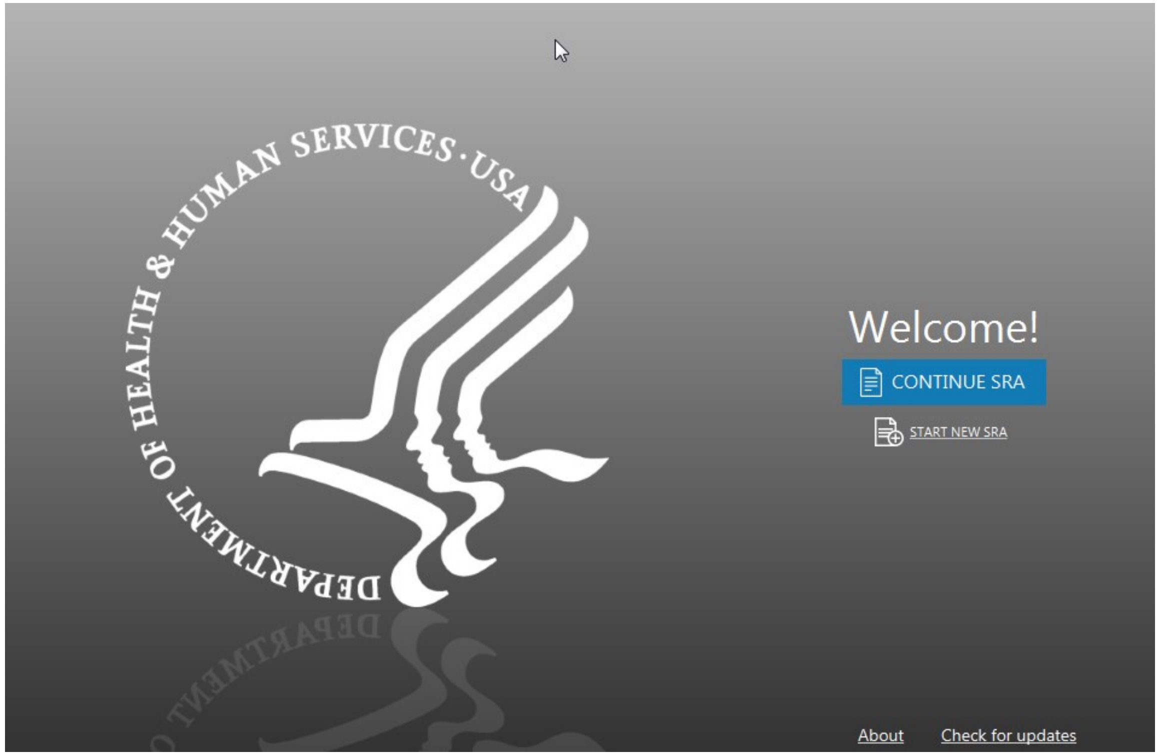
Download & Installation

The tool can be downloaded from [HealthIT.gov](https://www.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. <u>No information is transmitted to DHHS, ONC or OCR.</u>



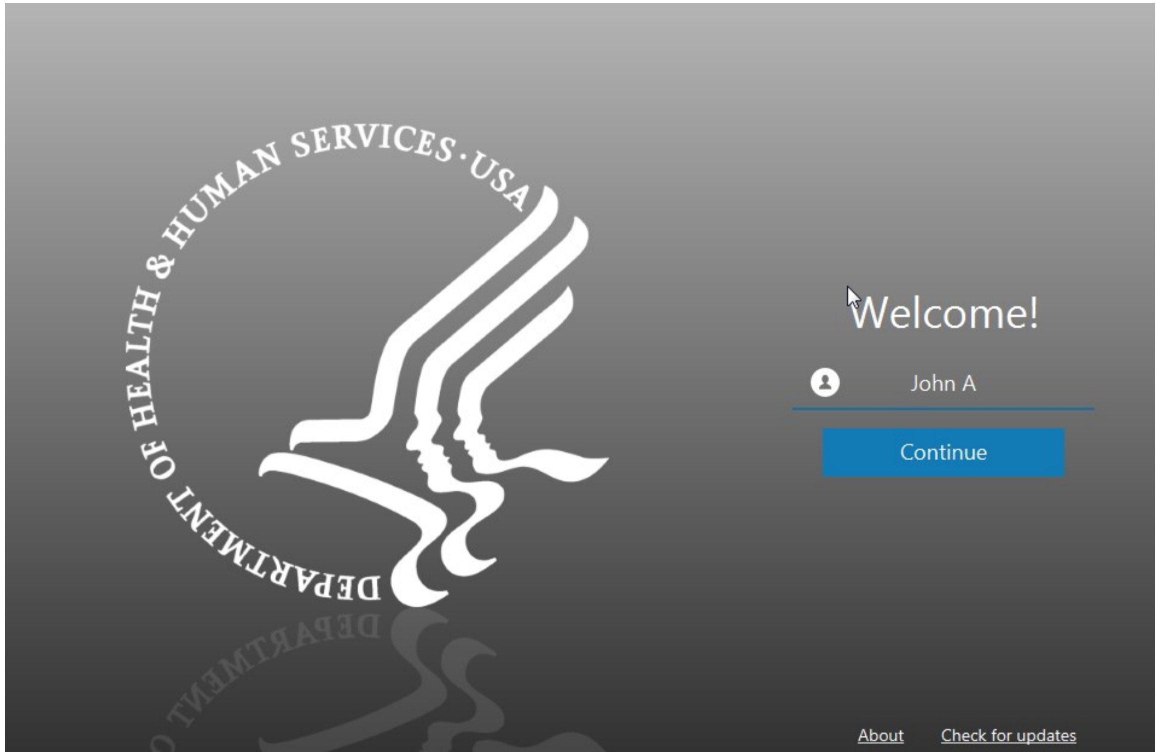
Welcome Screen

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.

Altarum

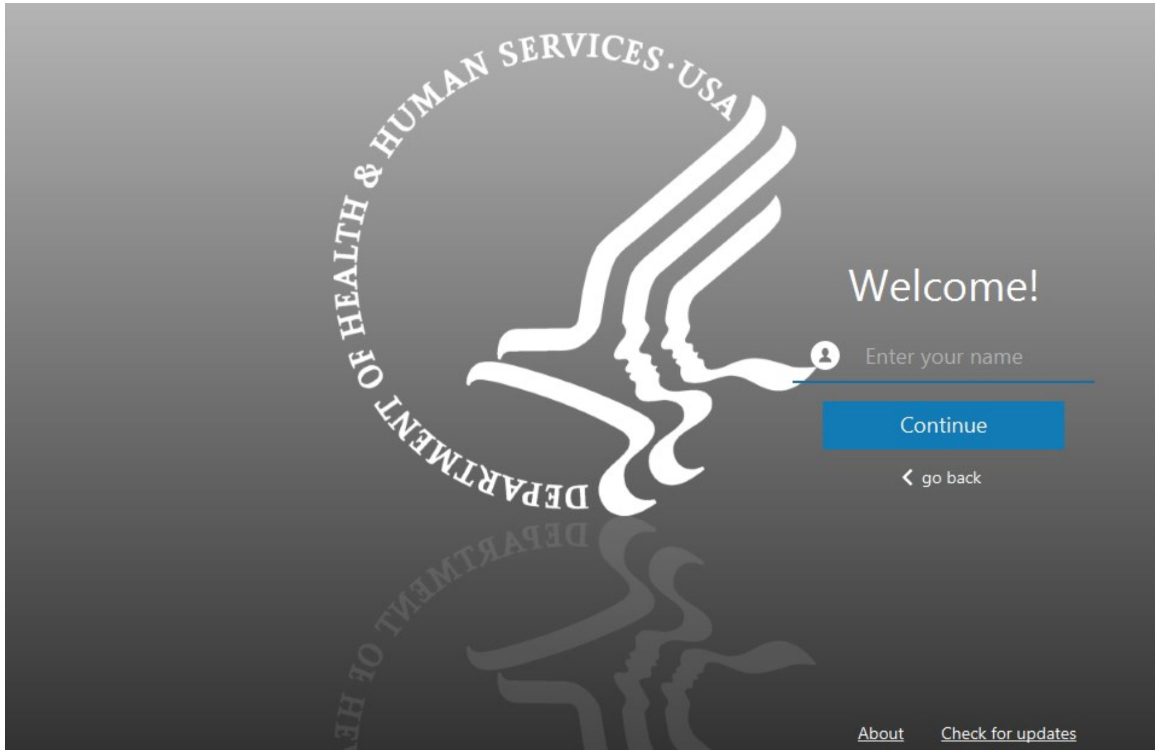


Entering a Username

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.

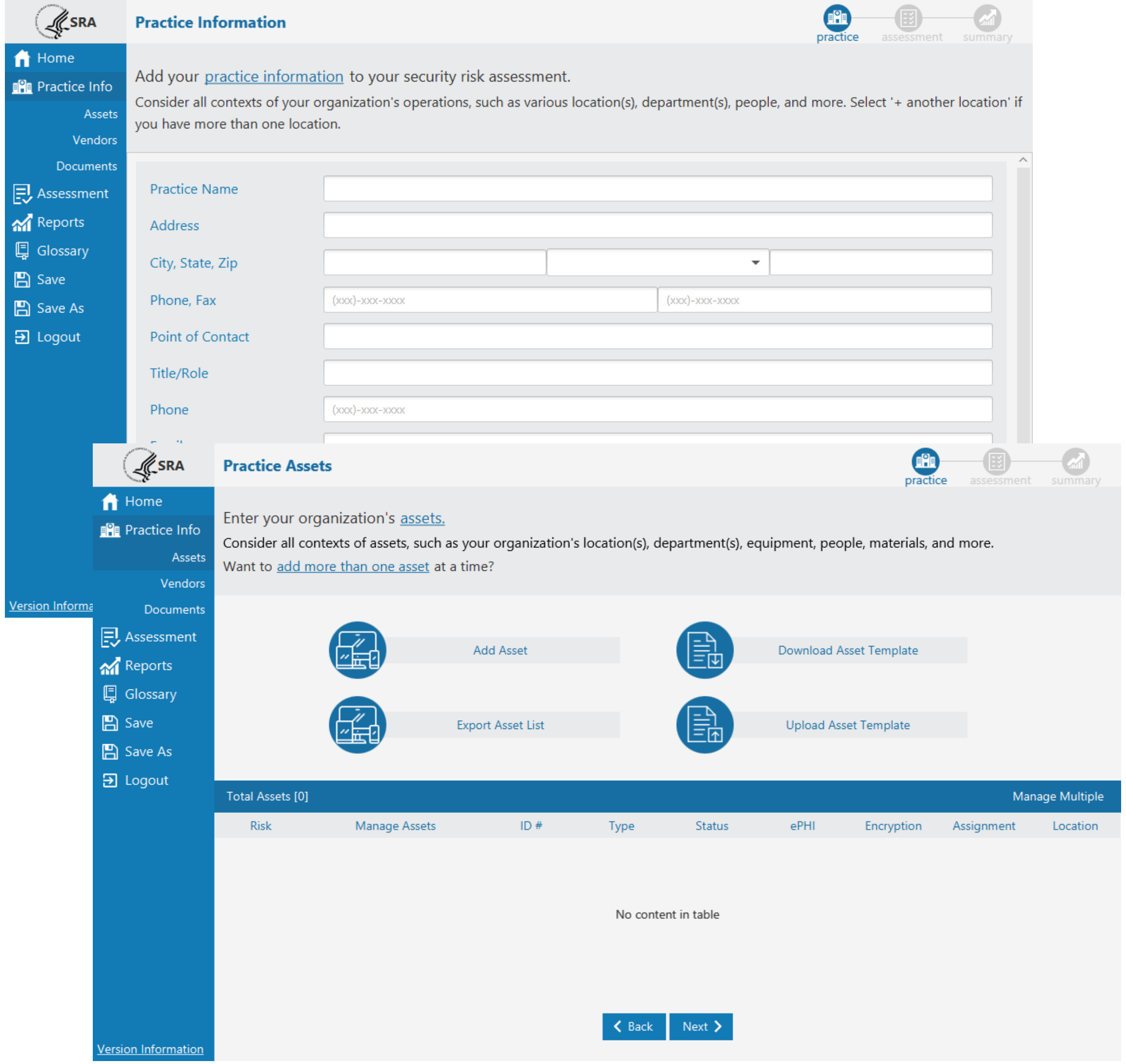


Saving a New SRA File

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.

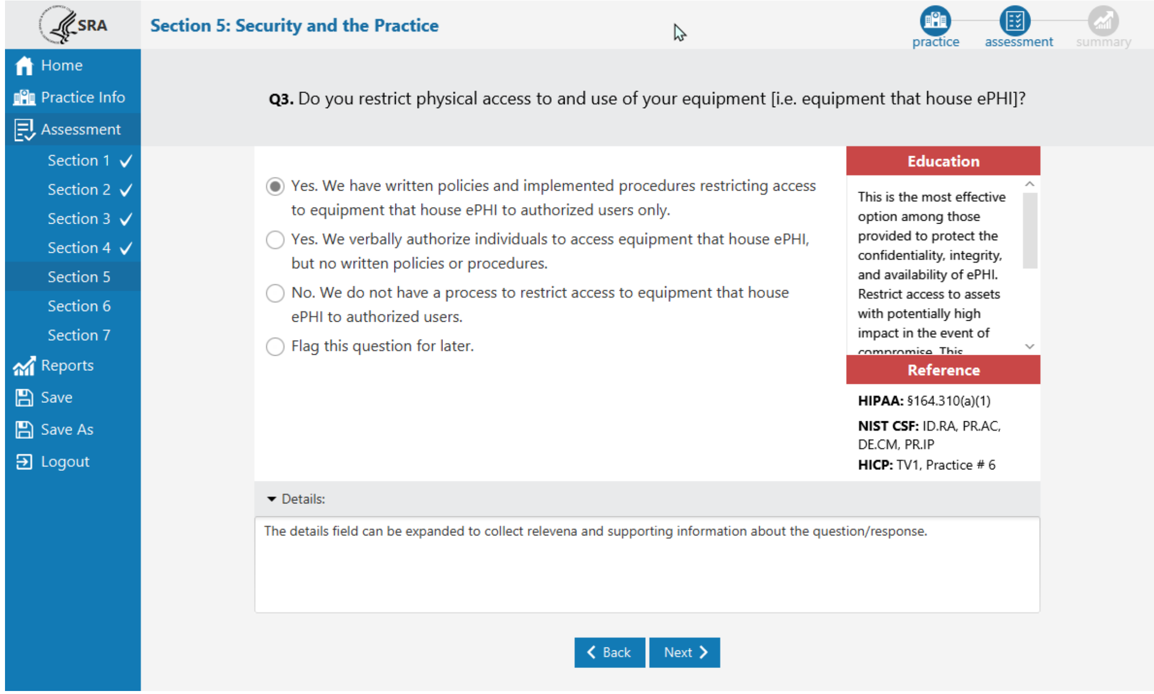


Practice Information, Asset & Vendor Management

A place to track:

- Practice locations
- Assets (computers, equipment, other hardware)
- Business Associates (vendors)
- Attached documents

Altarum



Assessment

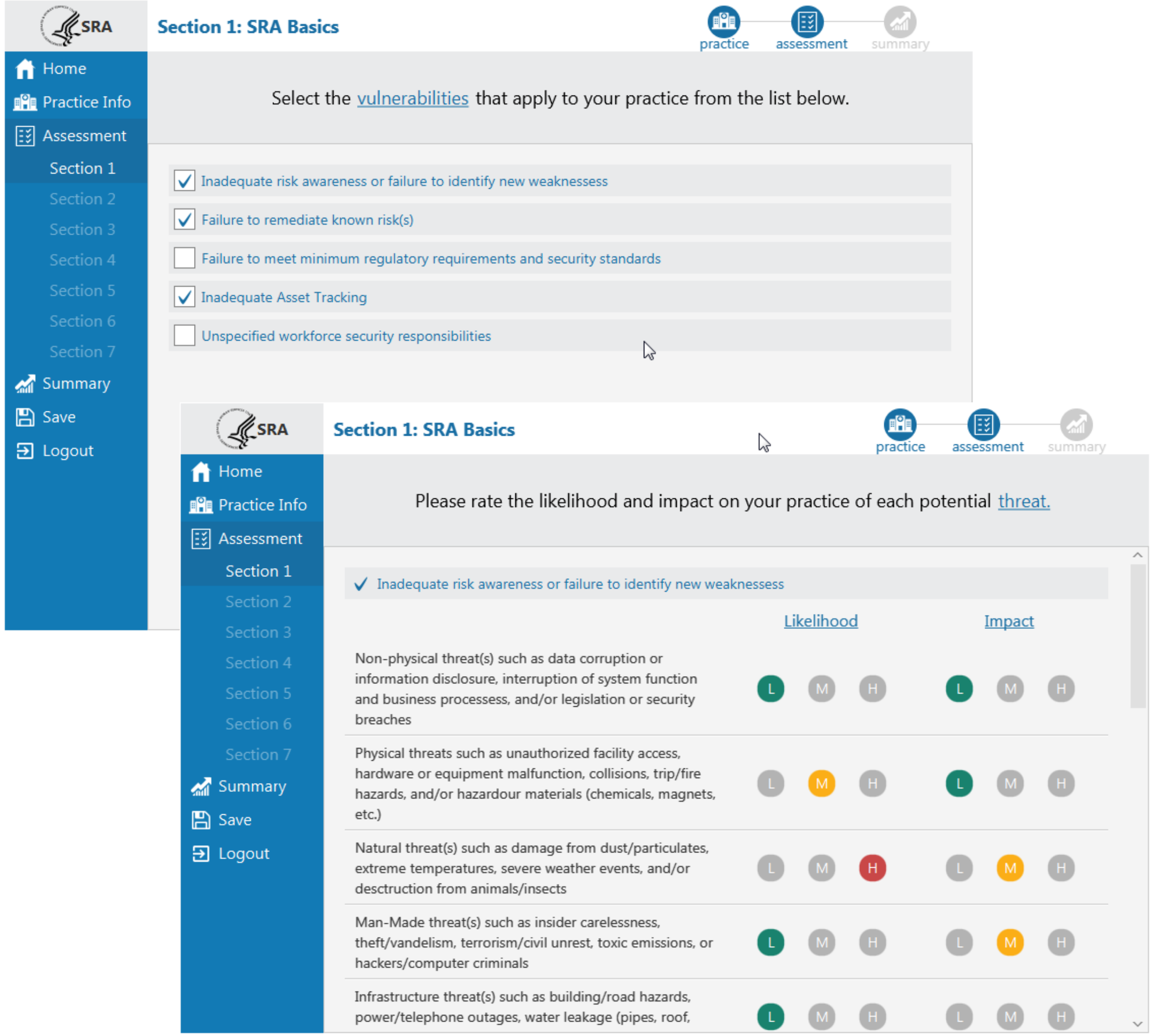
The Assessment section contains 7 sections with multiple-choice questions and branching logic.

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.

Altarum



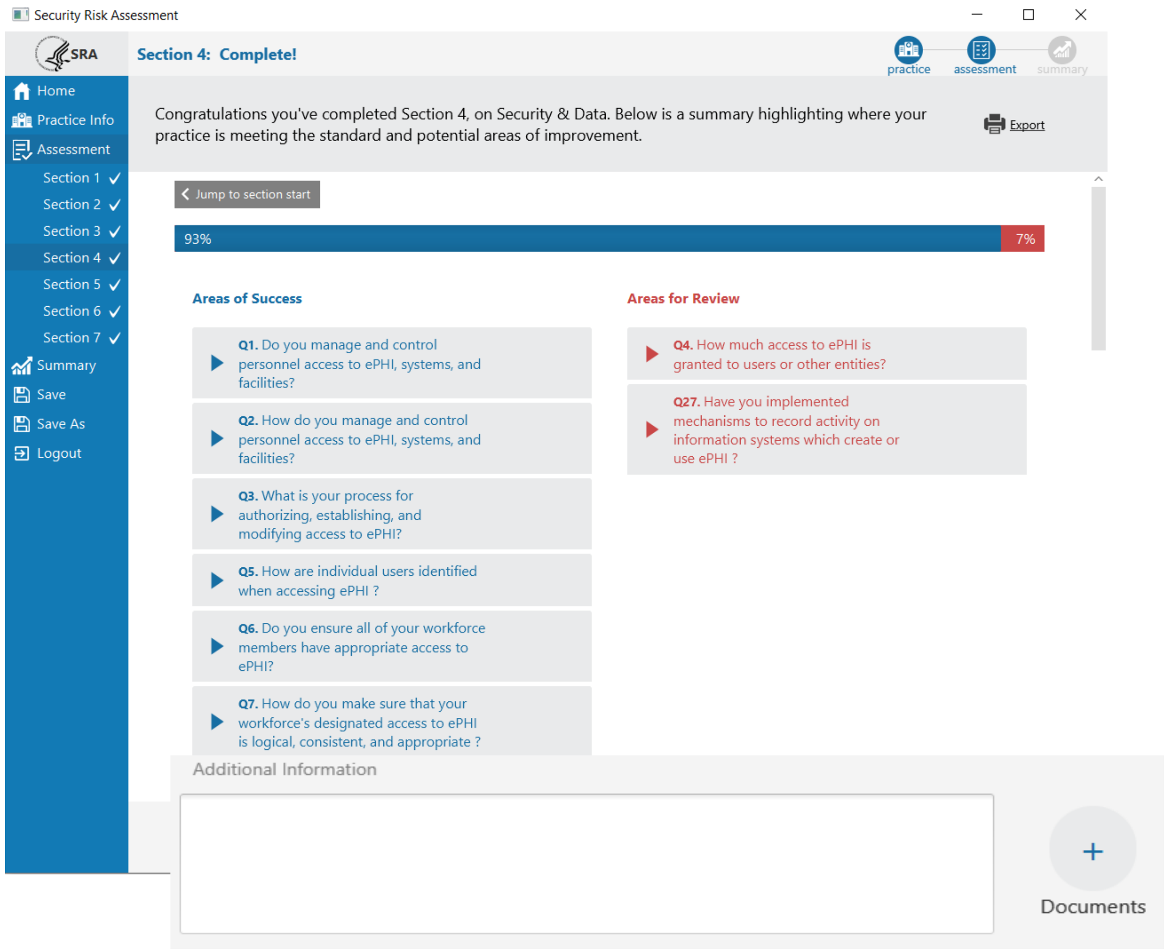
Threats & Vulnerabilities

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.

Altarum



Altarum

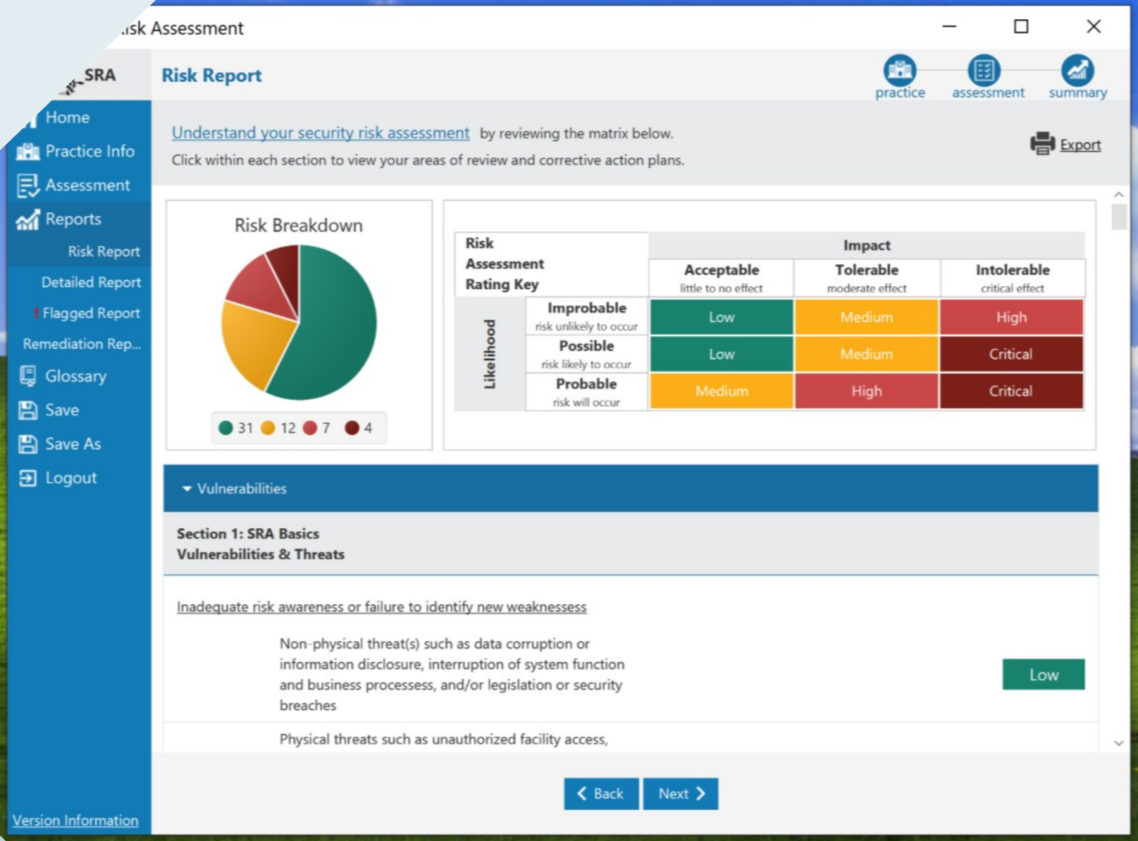
Section Summary

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.

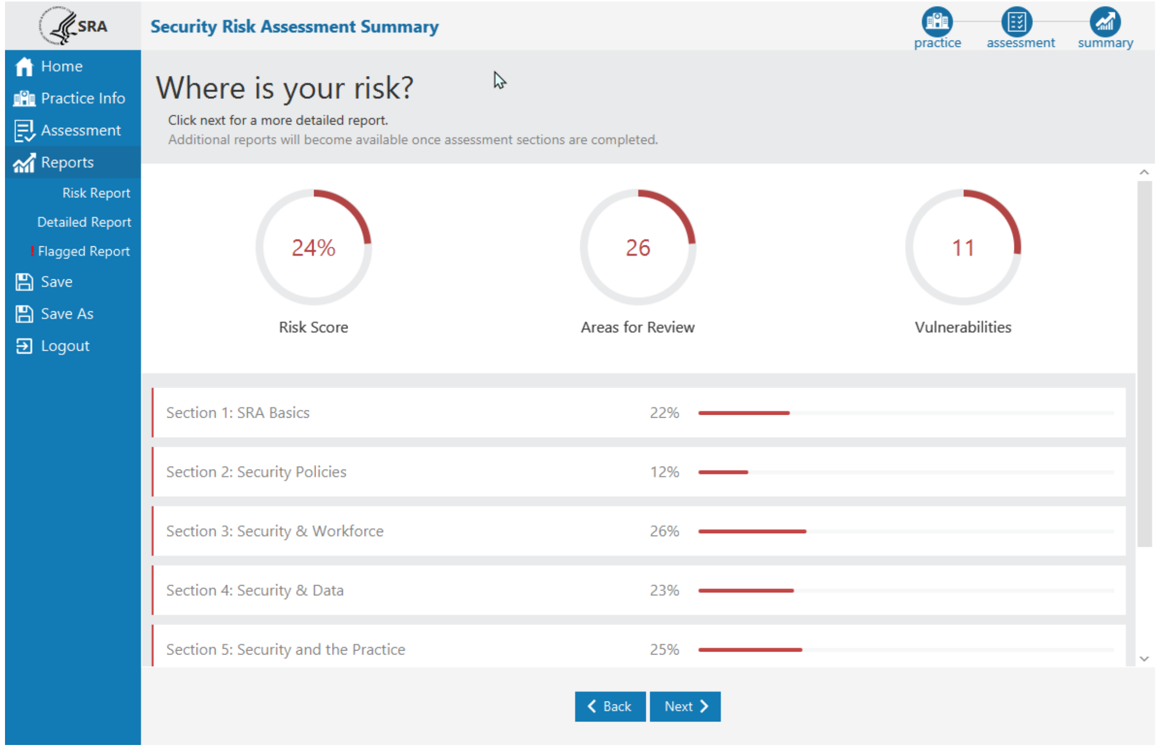
Users can enter **Additional Information** specific to each assessment section and add/link relevant documents necessary to demonstrate accuracy and thoroughness of responses.

Reports



isk Assessment
SRA
Risk Report
practice
assessment
summary
Home
Practice Info
Assessment
Reports
Risk Report
Detailed Report
Flagged Report
Remediation Rep...
Glossary
Save
Save As
Logout
Version Information
Understand your security risk assessment by reviewing the matrix below.
Click within each section to view your areas of review and corrective action plans.
Export
Risk Breakdown
31 12 7 4
Risk Assessment Rating Key
Impact
Acceptable
little to no effect
Tolerable
moderate effect
Intolerable
critical effect
Likelihood
Improbable
risk unlikely to occur
Low Medium High
Possible
risk likely to occur
Low Medium Critical
Probable
risk will occur
Medium High Critical
Vulnerabilities
Section 1: SRA Basics
Vulnerabilities & Threats
Inadequate risk awareness or failure to identify new weaknesses
Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches
Low
Physical threats such as unauthorized facility access,
Back
Next

Summary Report



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

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

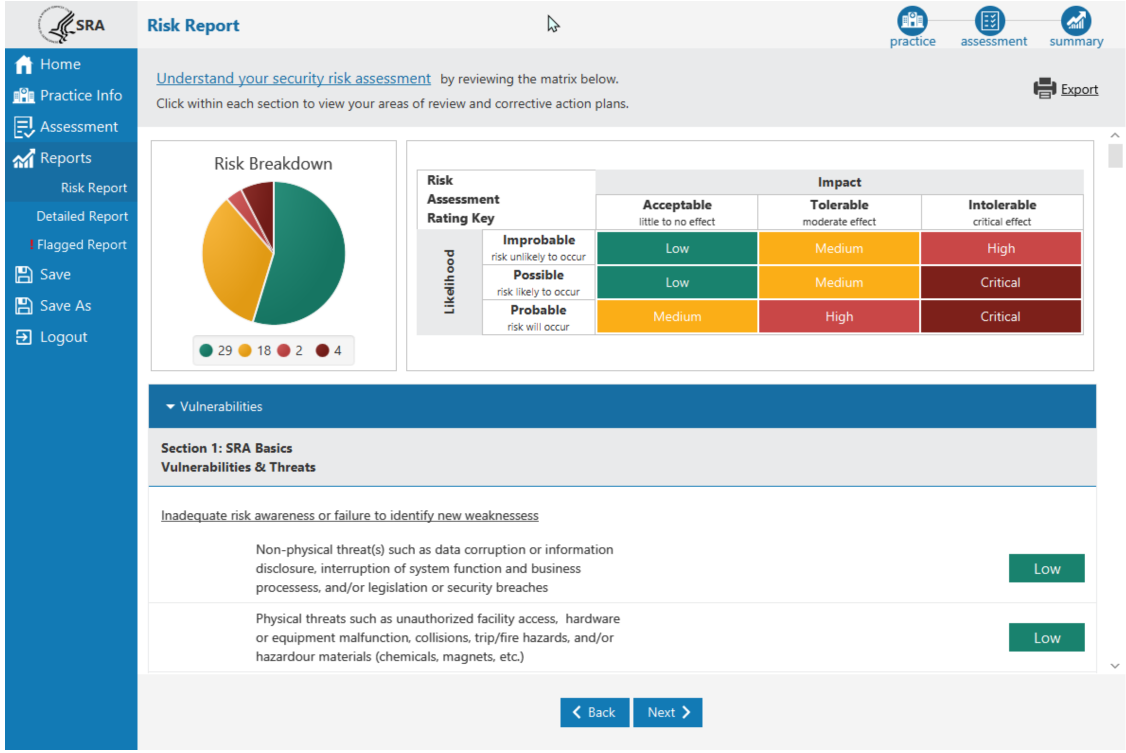
Risk Score – shows the number of questions sorted into Areas for Review divided by the total questions the user answered.

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.

Altarum



Risk Report

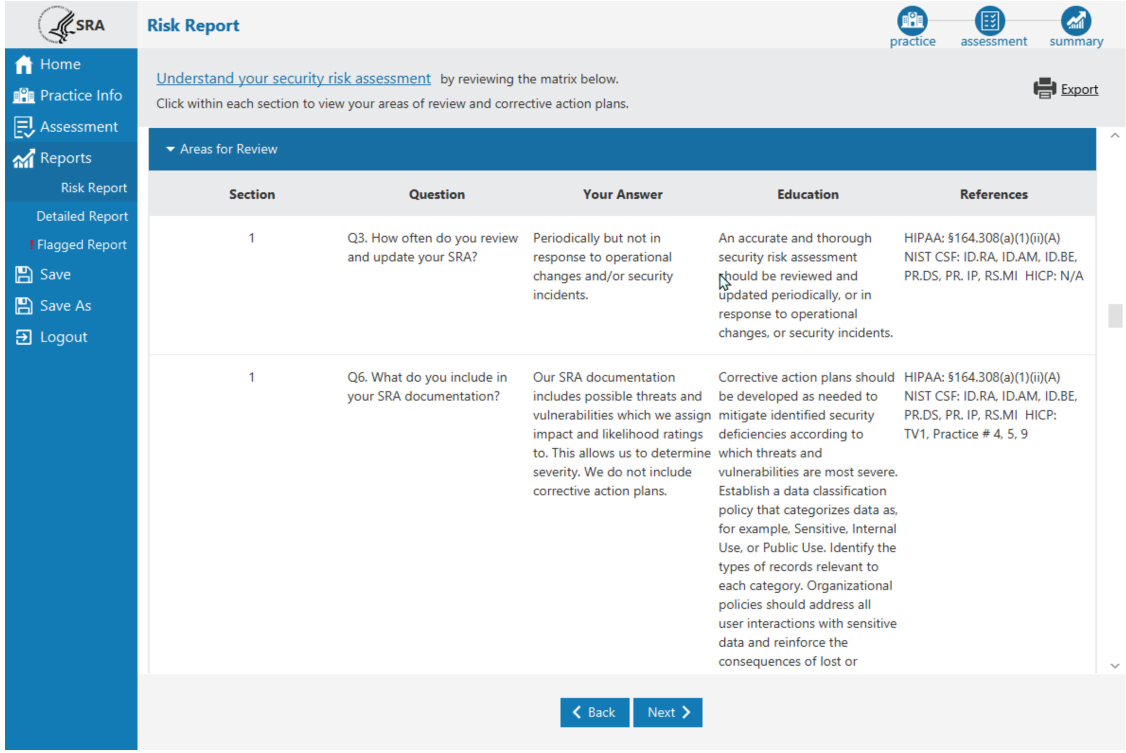
The Risk Report identifies all areas of risk collected across your entire assessment.

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.

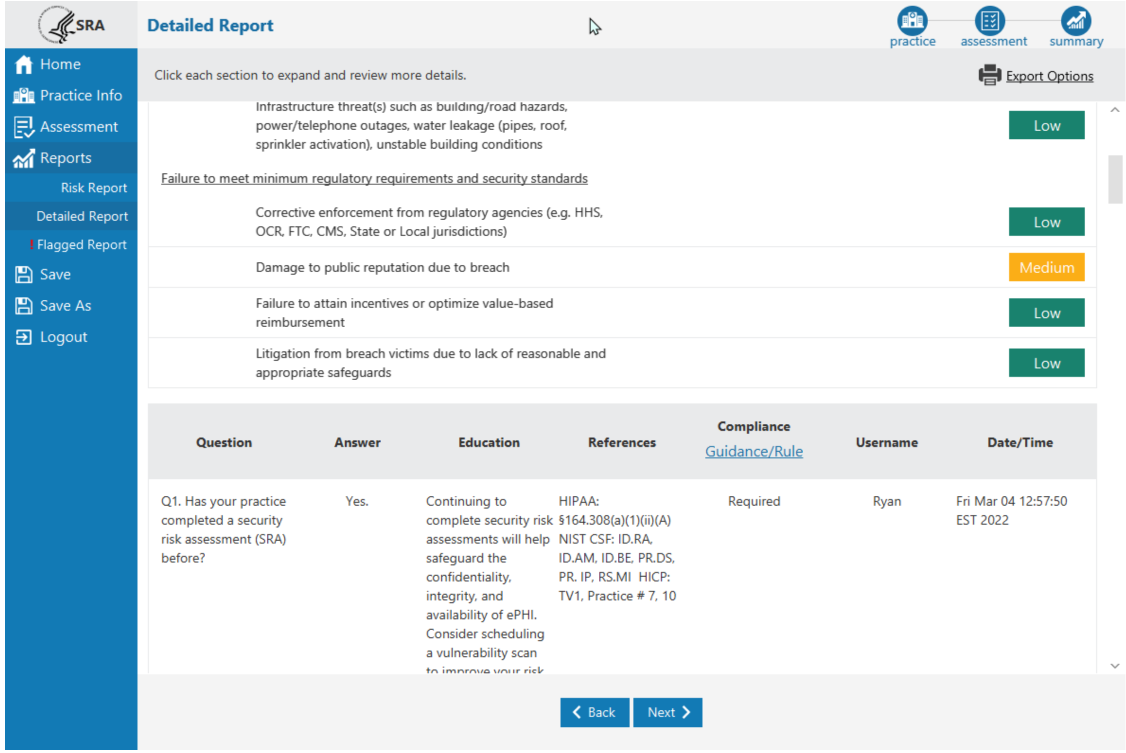
Altarum



Risk Report

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.



Detailed Report

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.

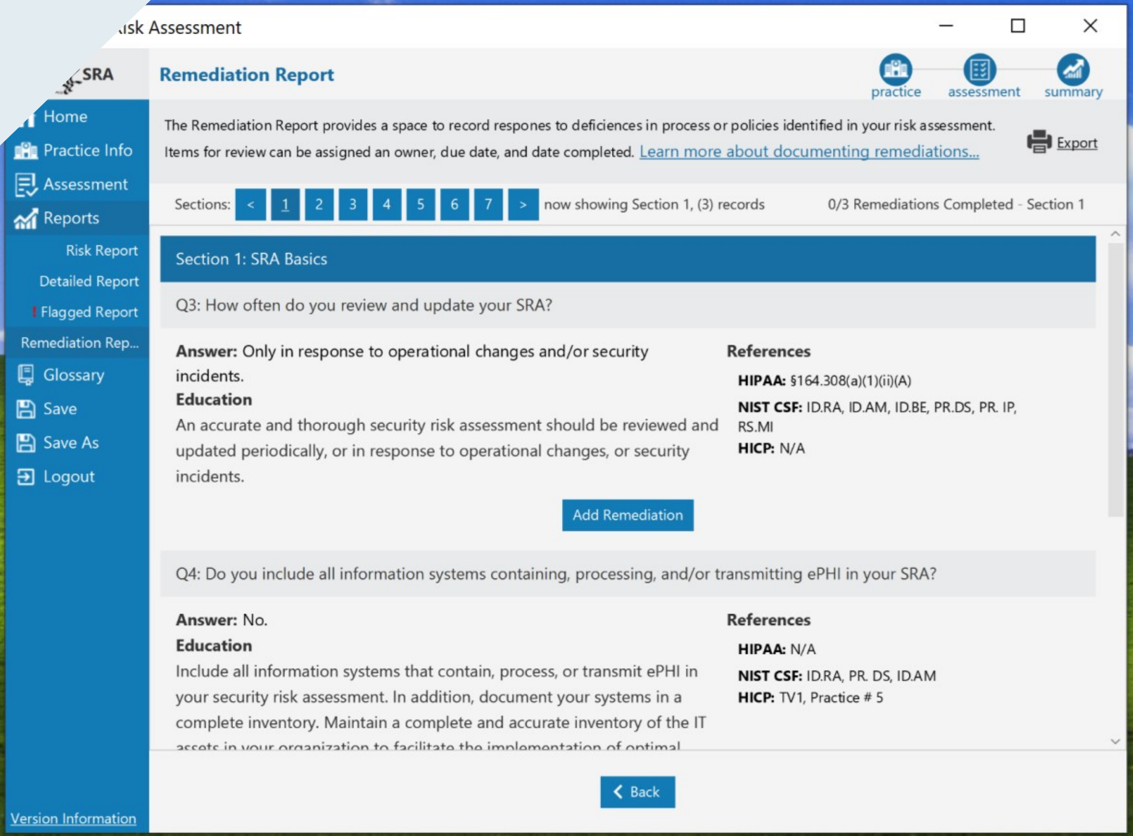
Export a PDF or Excel copy of the report using the Export Options button.

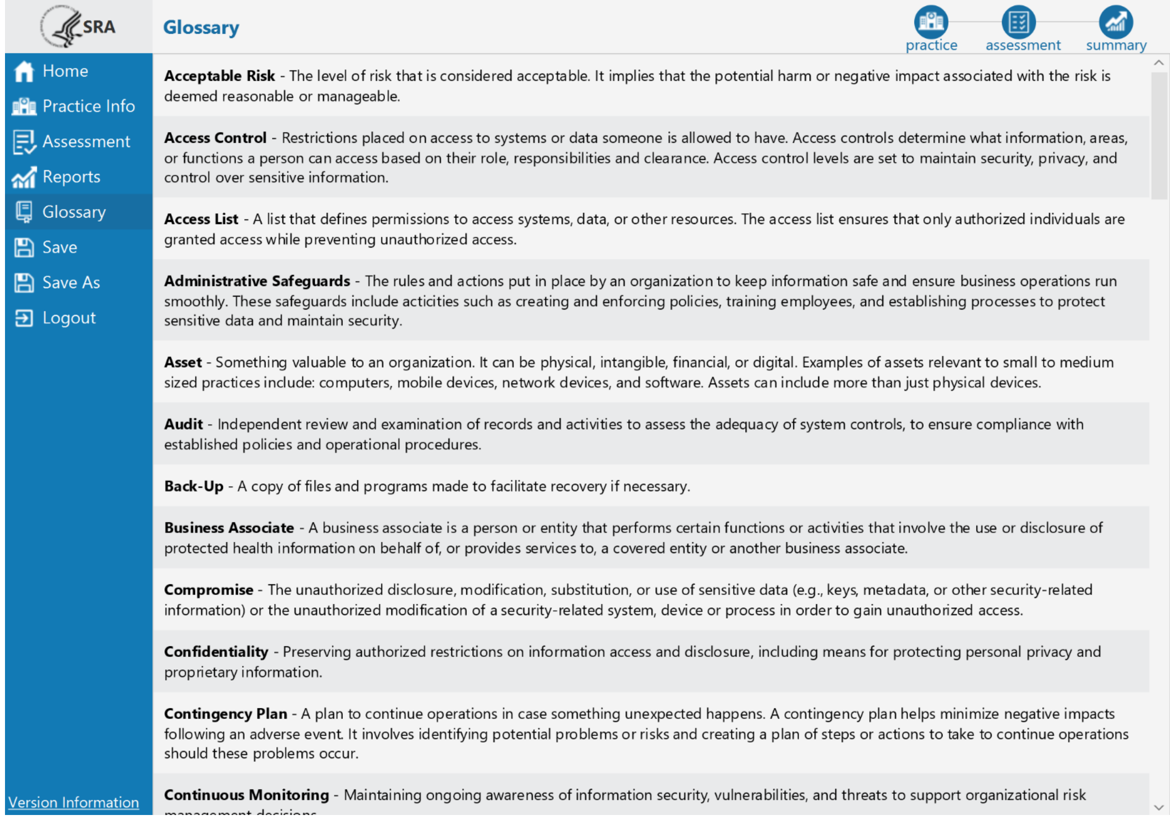
Altarum

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

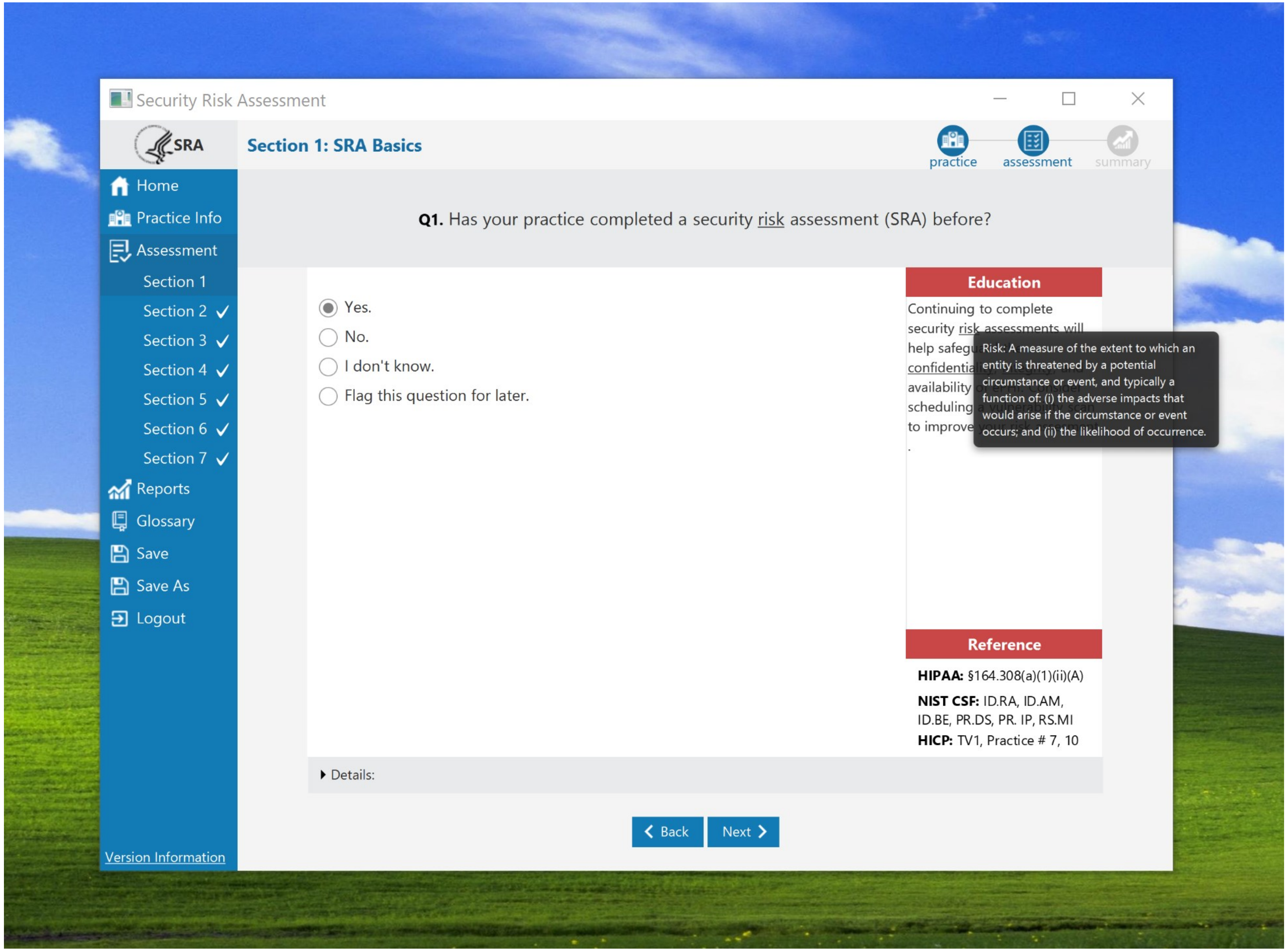




Glossary

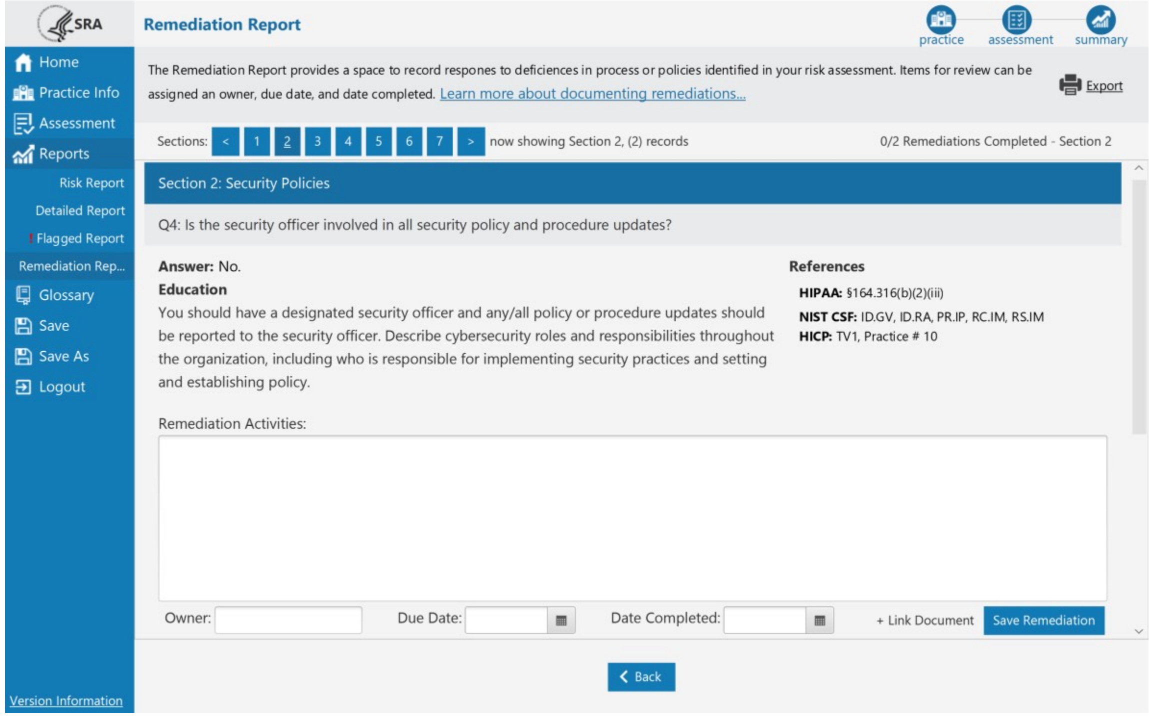
Glossary Page – terms and definitions provided in one place for easy access

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



Security Risk Assessment
SRA
Section 1: SRA Basics
practice
assessment
summary
Home
Practice Info
Assessment
Section 1
Section 2 ✓
Section 3 ✓
Section 4 ✓
Section 5 ✓
Section 6 ✓
Section 7 ✓
Reports
Glossary
Save
Save As
Logout
Version Information
Q1. Has your practice completed a security risk assessment (SRA) before?
Yes.
No.
I don't know.
Flag this question for later.
Education
Continuing to complete
security risk assessments will
help safegu
confidentia
availability
scheduling
to improve
Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Reference
HIPAA: §164.308(a)(1)(ii)(A)
NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI
HICP: TV1, Practice # 7, 10
Details:
Back
Next

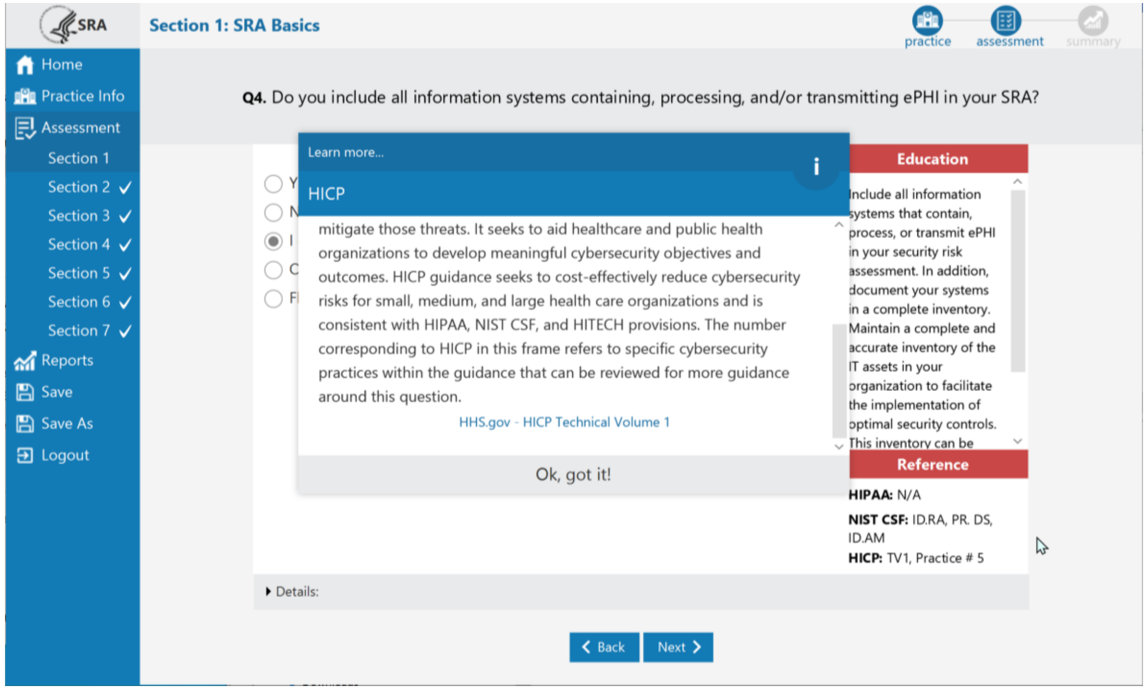
Remediation Report



- 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

Altarum

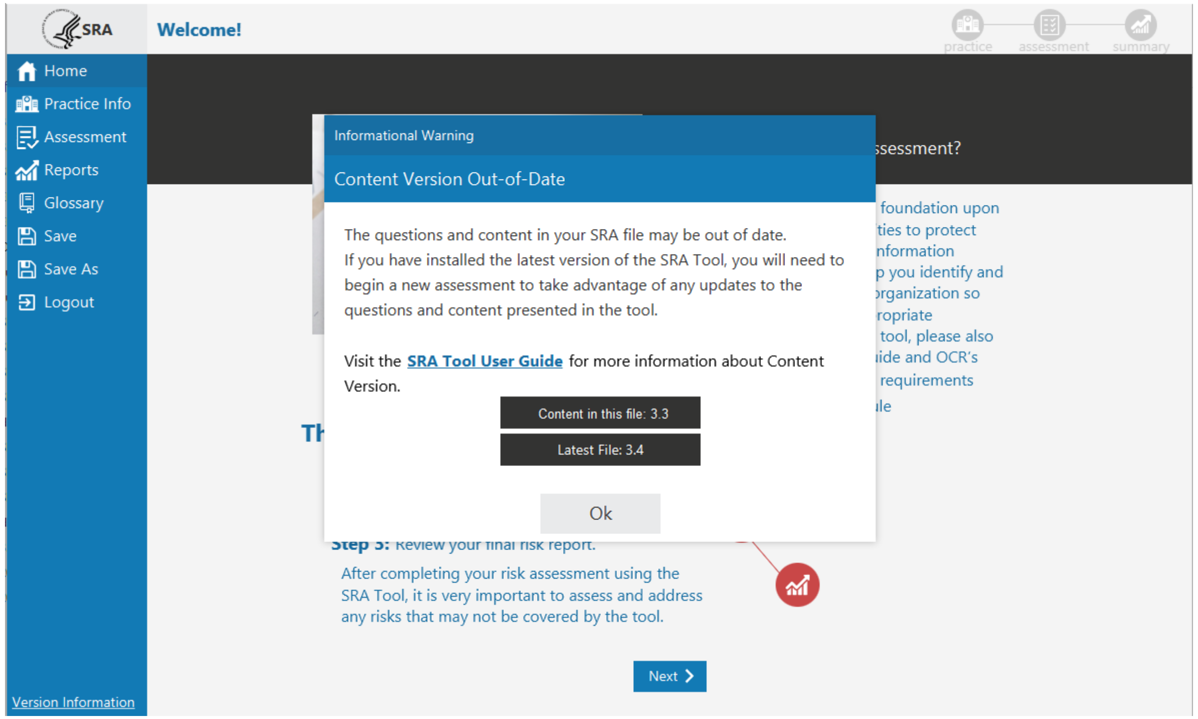
HICP 2023 Edition Updates



References updated for HICP 2023 Edition.

- New references added
- Links updated

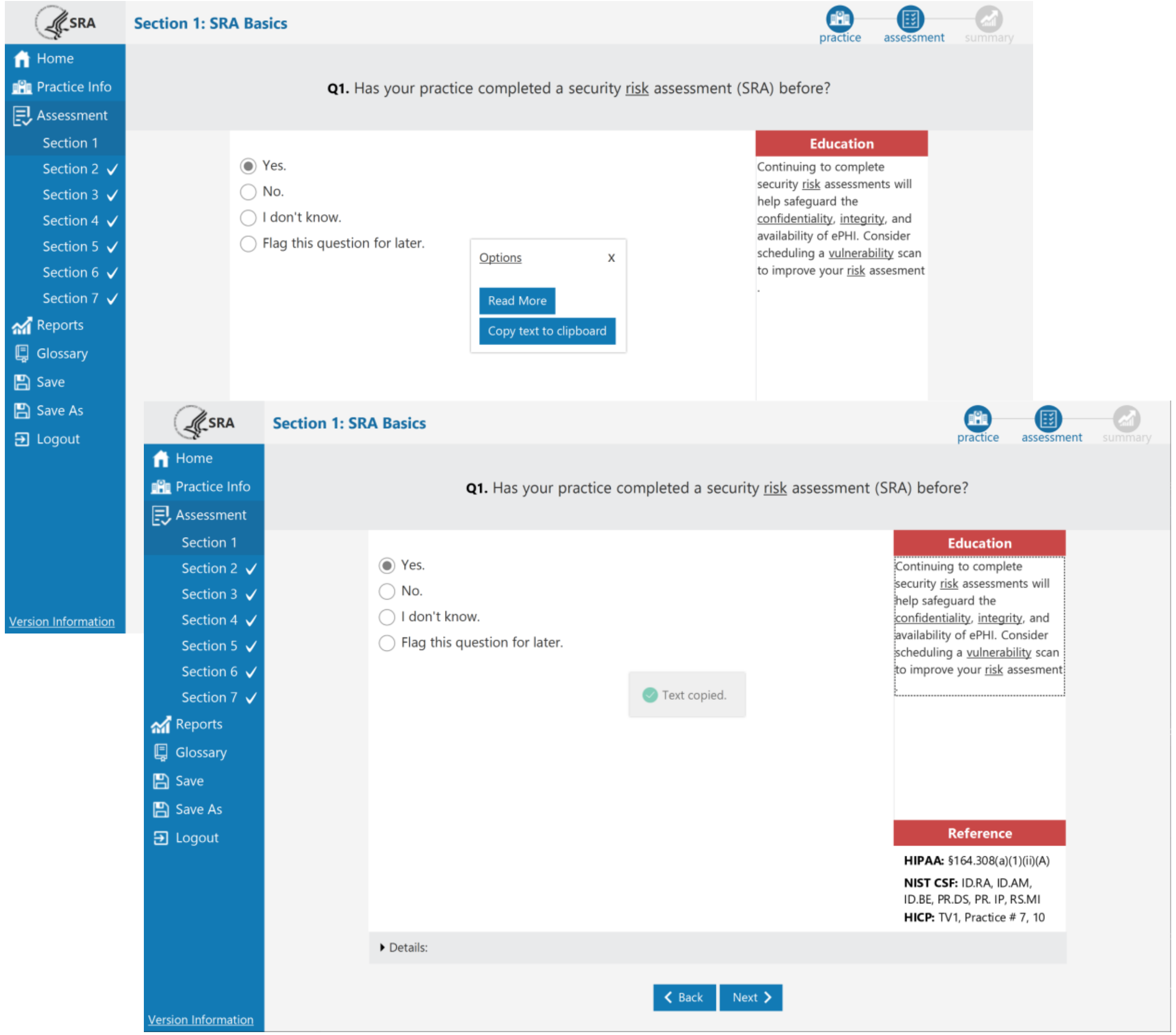
Altarum



Content Version Warning

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

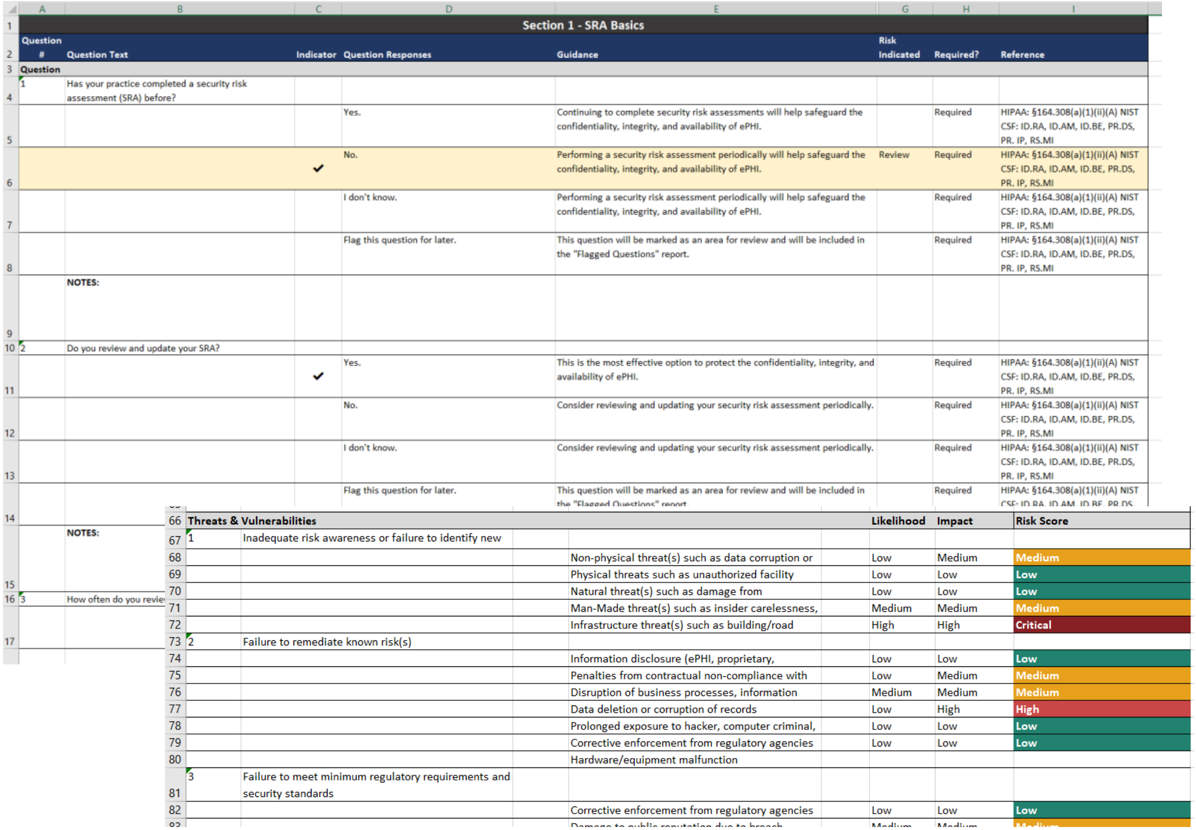
Must be dismissed each time old file is opened.



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

Altarum



Question #	Question Text	Indicator	Question Responses	Guidance	Risk Indicated	Required?	Reference
Section 1 - SRA Basics							
Question							
1	Has your practice completed a security risk assessment (SRA) before?						
			Yes.	Continuing to complete security risk assessments will help safeguard the confidentiality, integrity, and availability of ePHI.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI
		✔	No.	Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI.	Review	Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI
			I don't know.	Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI
			Flag this question for later.	This question will be marked as an area for review and will be included in the "Flagged Questions" report.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI
	NOTES:						
2	Do you review and update your SRA?						
		✔	Yes.	This is the most effective option to protect the confidentiality, integrity, and availability of ePHI.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI
			No.	Consider reviewing and updating your security risk assessment periodically.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI
			I don't know.	Consider reviewing and updating your security risk assessment periodically.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI
			Flag this question for later.	This question will be marked as an area for review and will be included in the "Flagged Questions" report.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS
	NOTES:						
3	How often do you revie						

Threats & Vulnerabilities			Likelihood	Impact	Risk Score
1	Inadequate risk awareness or failure to identify new				
		Non-physical threat(s) such as data corruption or	Low	Medium	Medium
		Physical threats such as unauthorized facility	Low	Low	Low
		Natural threat(s) such as damage from	Low	Low	Low
		Man-Made threat(s) such as insider carelessness,	Medium	Medium	Medium
		Infrastructure threat(s) such as building/road	High	High	Critical
2	Failure to remediate known risk(s)				
		Information disclosure (ePHI, proprietary,	Low	Low	Low
		Penalties from contractual non-compliance with	Low	Medium	Medium
		Disruption of business processes, information	Medium	Medium	Medium
		Data deletion or corruption of records	Low	High	High
		Prolonged exposure to hacker, computer criminal,	Low	Low	Low
		Corrective enforcement from regulatory agencies	Low	Low	Low
		Hardware/equipment malfunction			
3	Failure to meet minimum regulatory requirements and security standards				
		Corrective enforcement from regulatory agencies	Low	Low	Low

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.

Altarum

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.

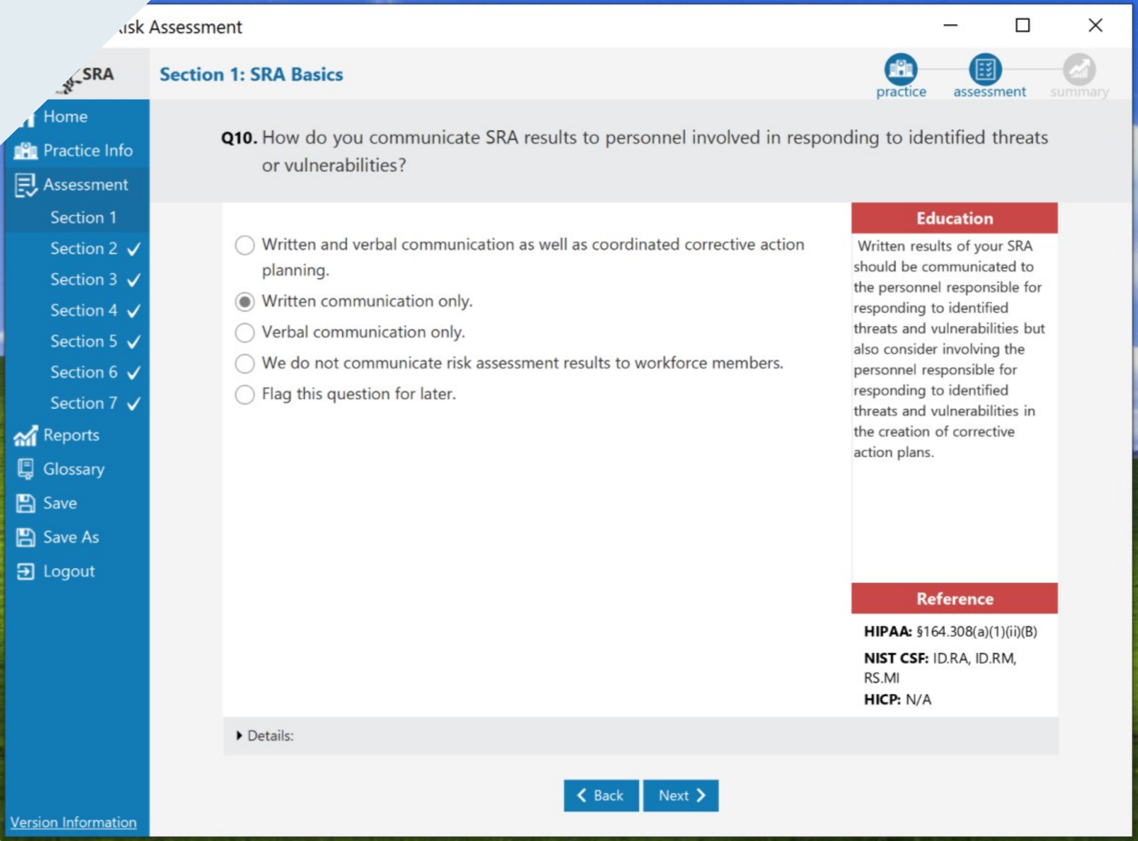
Is SRA Tool available for Apple or Mac computers?

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 HealtIT.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