

SRA TOOL | OVERVIEW AND NEW FEATURES

Presenter: Ryan Callahan

Panelists: Nick Heesters [OCR], Ali Massihi [ONC], Kathleen Pisa [Altarum]



Agenda

Security Risk Assessment Tool

- Overview of the SRA Tool
- Downloading, installing, and using the SRA Tool

Updating your assessment

New Features

Q&A

How to Get More Information

- SRA Tool Training video and User Guide
- How to Contact the SRA Helpdesk



Overview of the SRA Tool



What is the SRA Tool?



Security Risk Assessment

Section 1: SRA Basics

practice assessment summary

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 safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk assessment.

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 >

4:37 PM
6/22/2022

Content



The SRA Tool's content was developed using the following sources:

- HIPAA Security Rule
- National Institute of Standards and Technology (NIST) Special Publication 800-66
- NIST Special Publication [Guide to Implementing FISMA Security Controls] 800-53
- NIST Special Publication [Guide to Assessing FISMA Controls] 800-53A
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Assessment questions will reference NIST Cybersecurity Framework guidance
- Health Industry Cybersecurity Practices (HICP)

Downloading, Installing, and Using the SRA Tool



Downloading and Installing the Tool



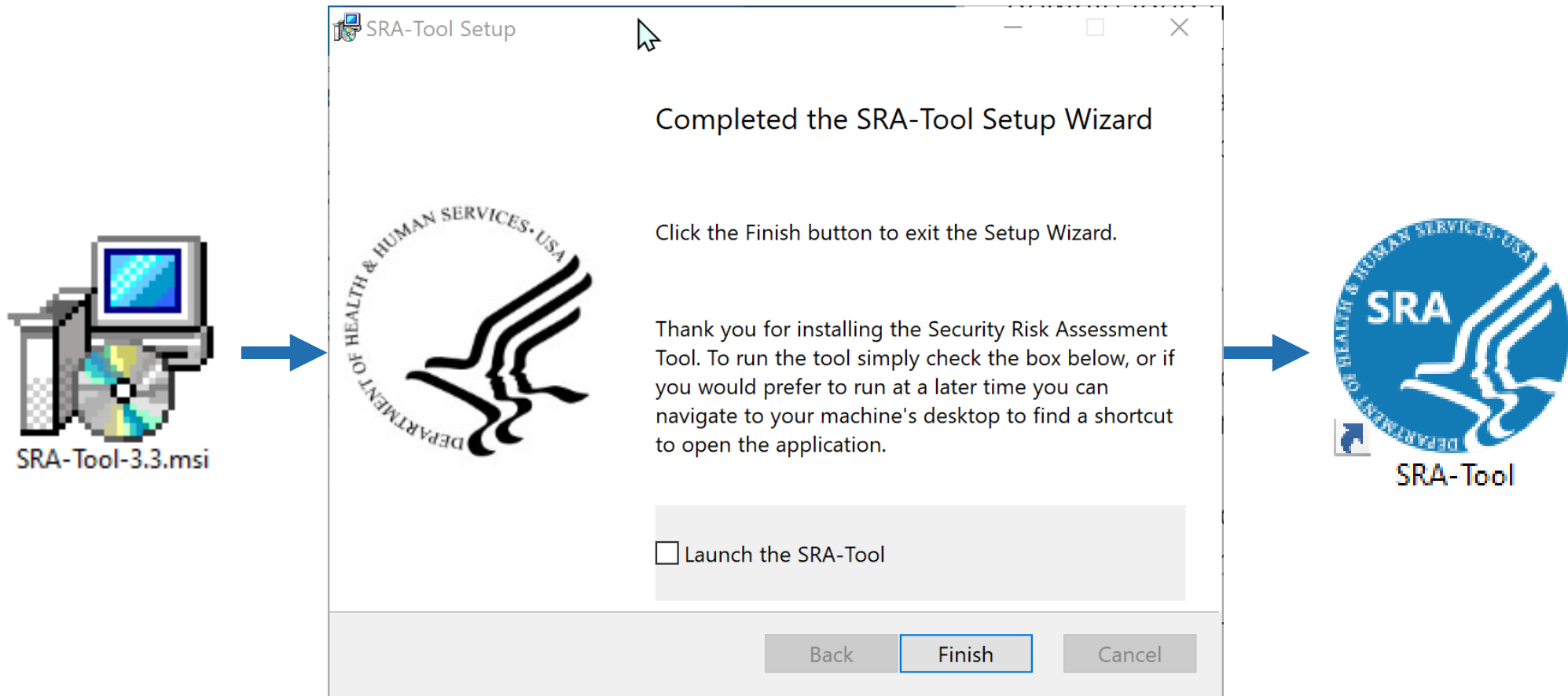
The screenshot shows the HealthIT.gov website. The header includes the HealthIT.gov logo, the text "Official Website of The Office of the National Coordinator for Health Information Technology (ONC)", and navigation links for TOPICS, BLOG, NEWS, DATA, and ABOUT ONC. A search bar is also present. The main content area is titled "Security Risk Assessment Tool" and includes a sidebar with links to Privacy, Security, and HIPAA resources. The main text explains the purpose of the tool and provides a download link for Version 3.3 of the SRA Tool for Windows (.msi - 70.3 MB).

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. No information is transmitted to DHHS, ONC or OCR.

Downloading and Installing the Tool



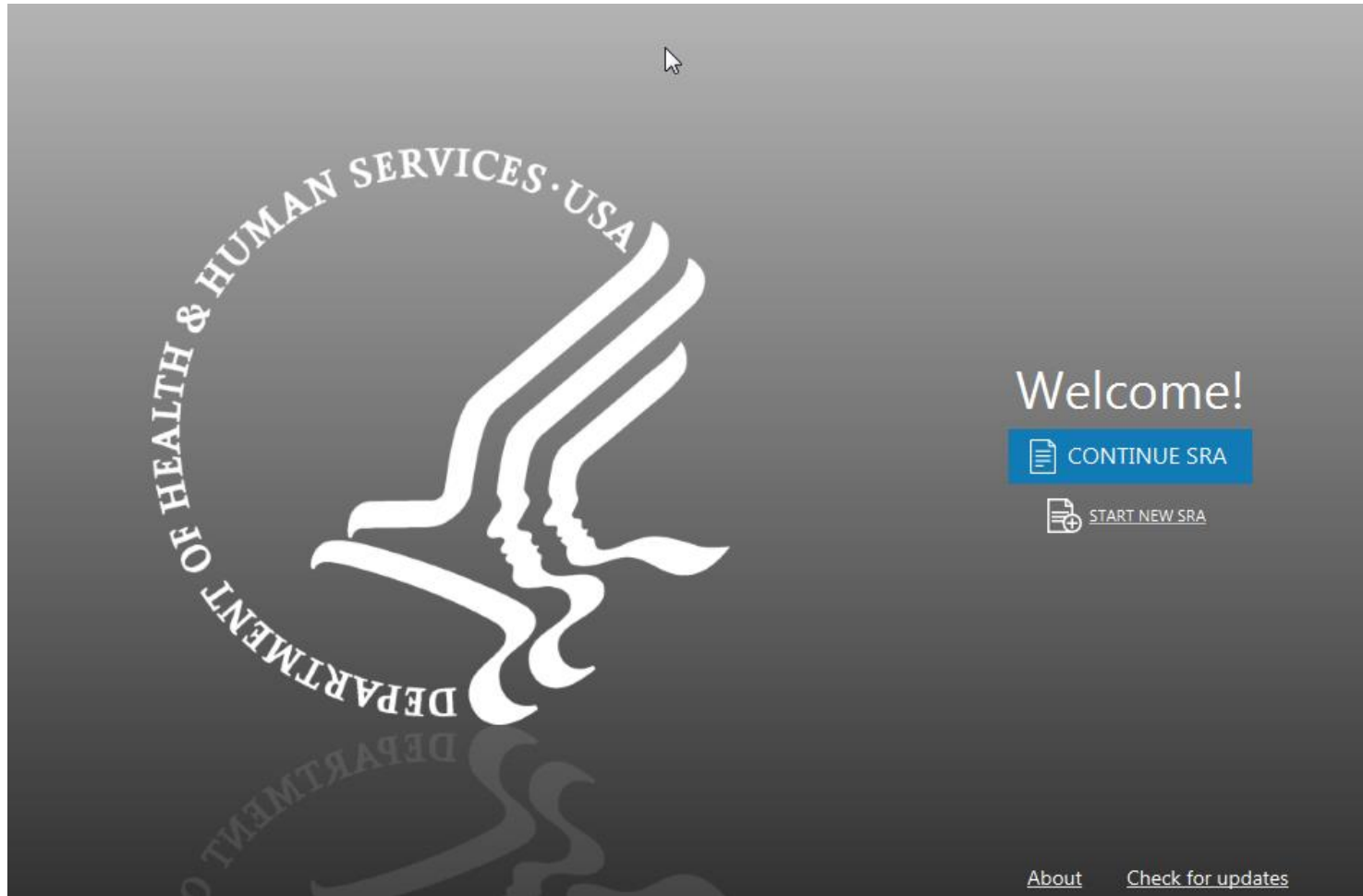
Starting a New Security Risk Assessment



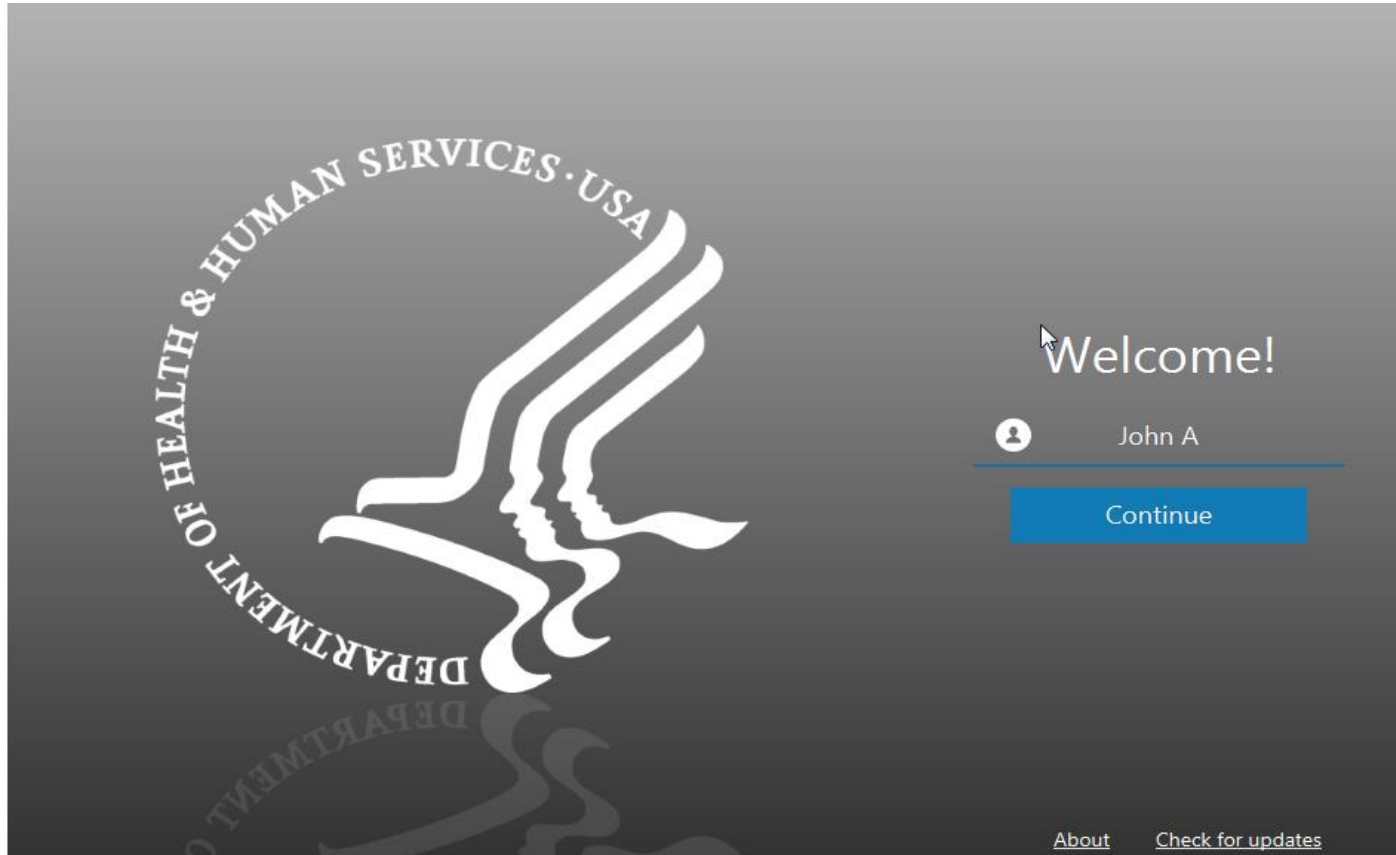
Select “Start New SRA” or “Continue SRA” to begin using the tool.

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.



Enter 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.

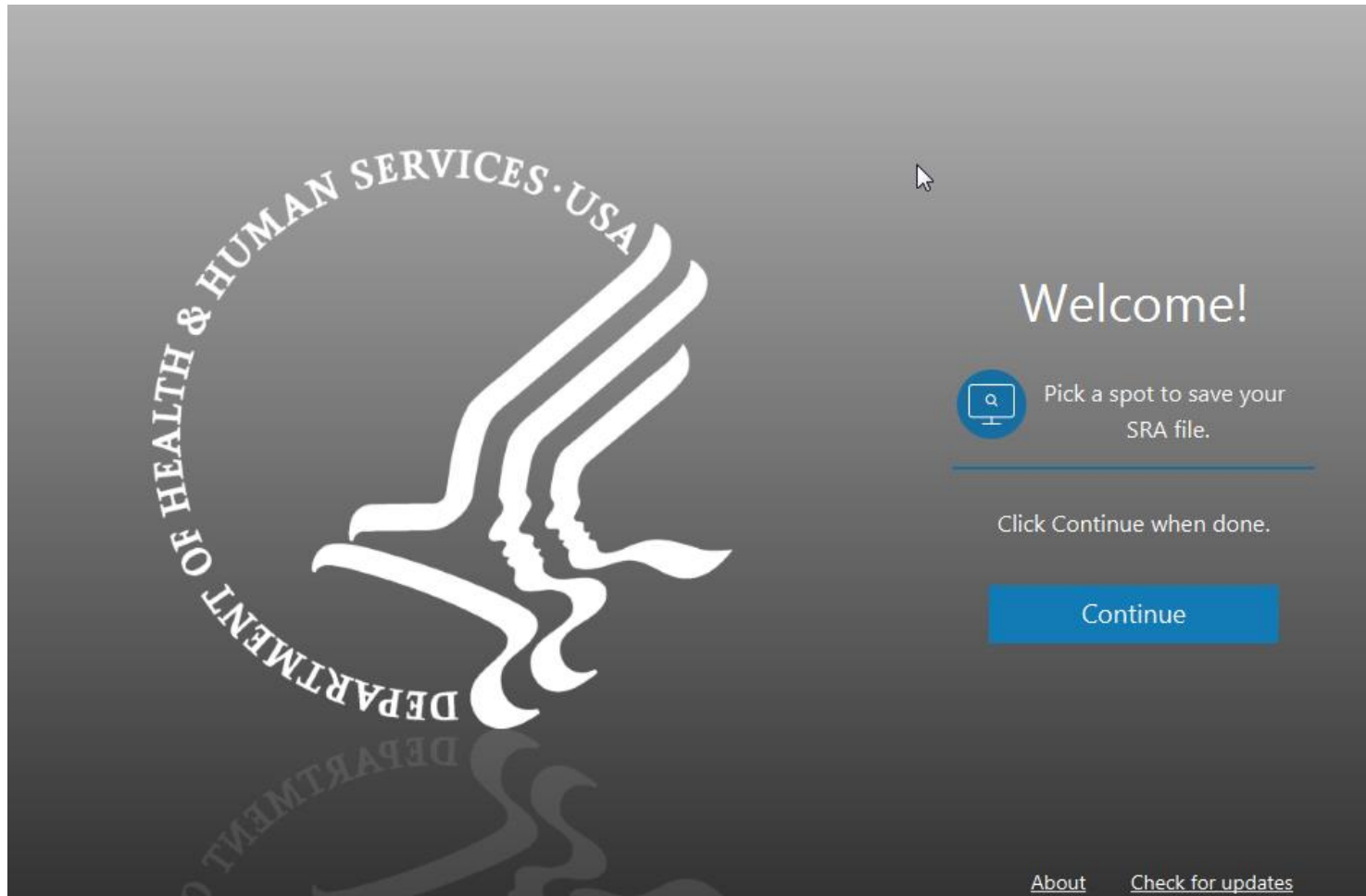
Saving Your Security Risk Assessment



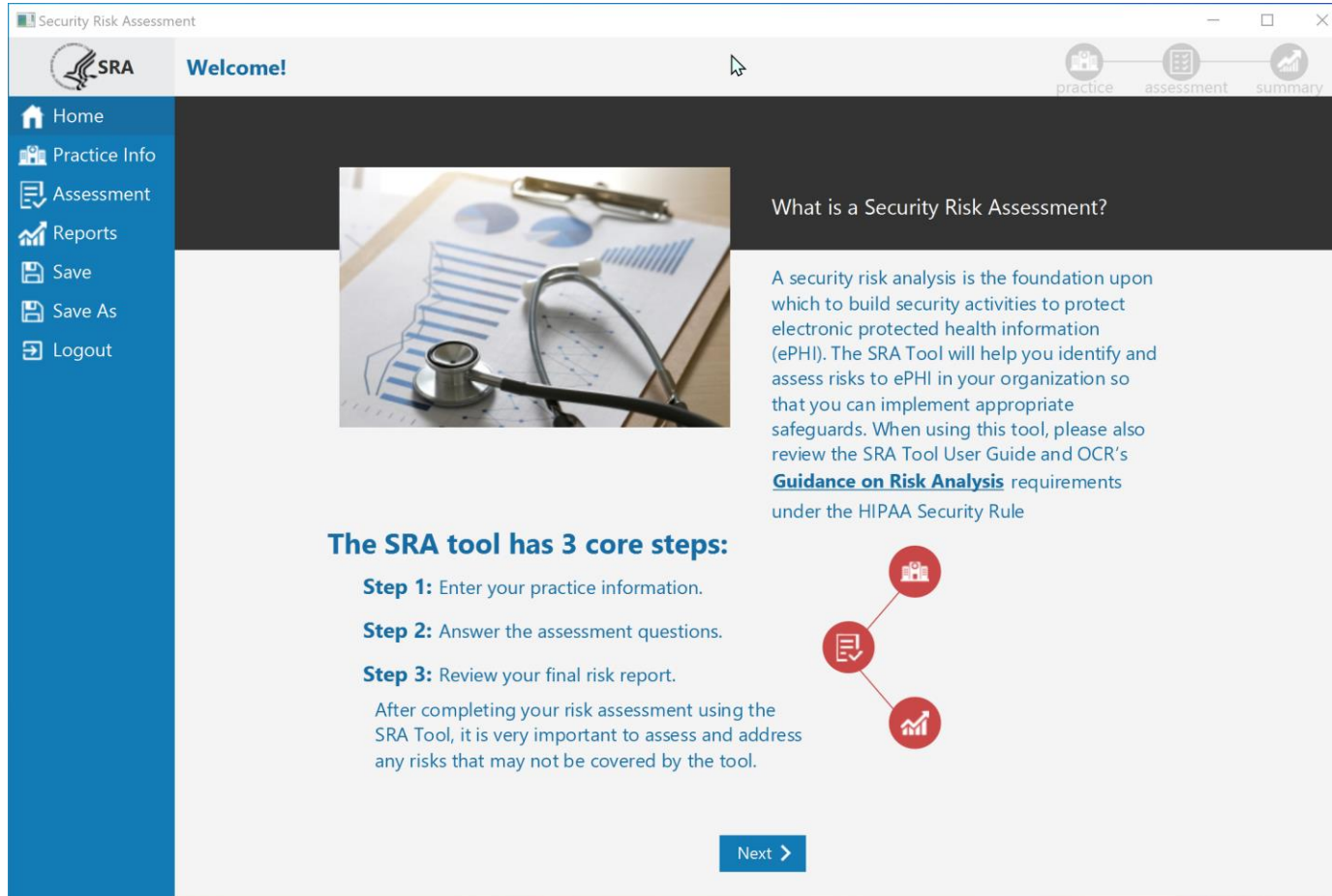
The SRA Tool is set up to work similar to Windows Office programs in the way it saves and opens assessment files.

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.



Starting an SRA

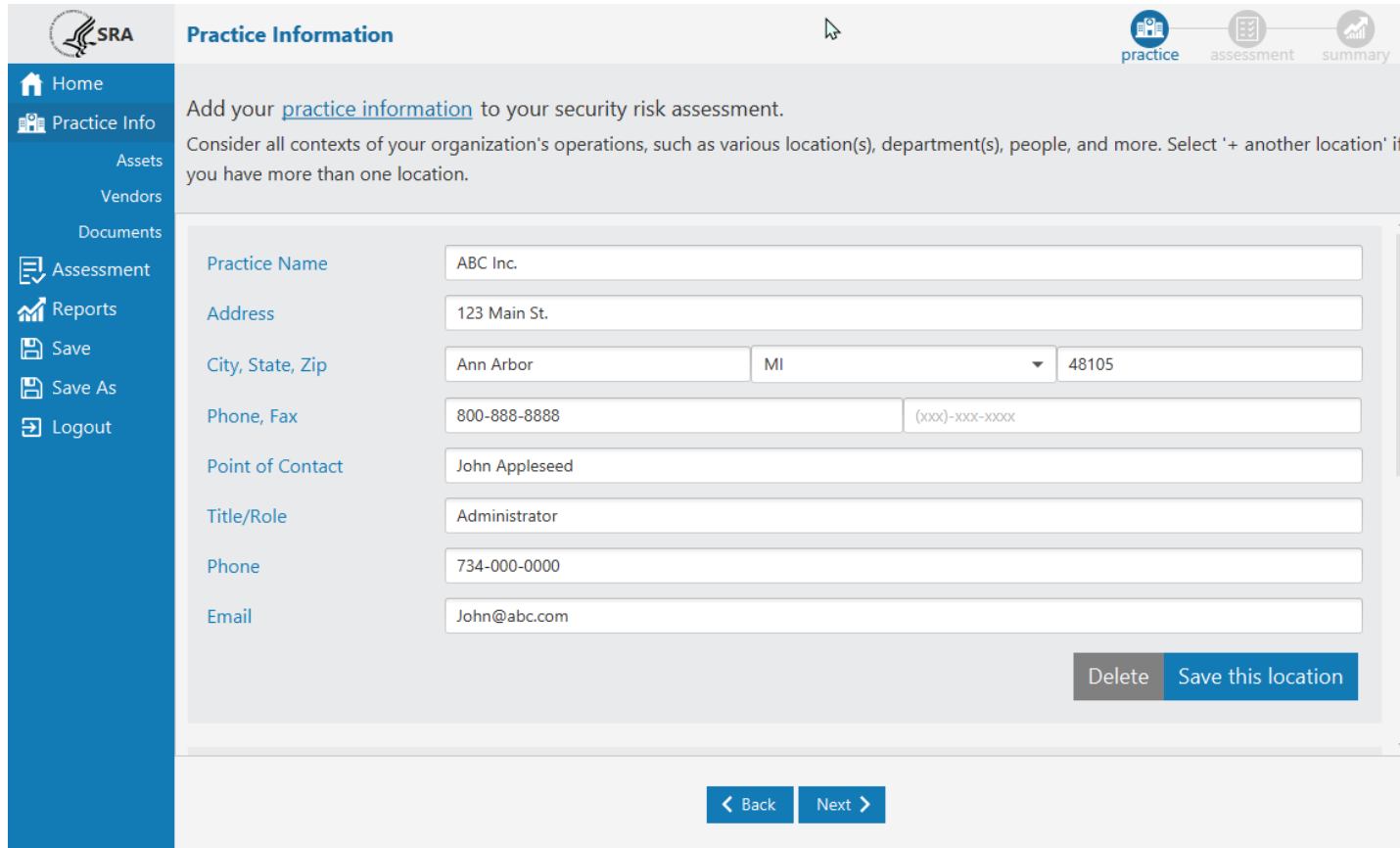


Navigation is handled using the **Next** and **Back** buttons at the bottom of each screen.

The left navigation menu allows users to jump between certain sections of the assessment and report, but due to branching logic, some navigation relies solely on the use of the Next/Back buttons.

The Summary item will not become available until the rest of the assessment has been fully completed.

Entering Practice Information



The screenshot shows the 'Practice Information' form in the SRA application. The left sidebar contains navigation links: Home, Practice Info, Assets, Vendors, Documents, Assessment, Reports, Save, Save As, and Logout. The main content area has a header with the SRA logo and the title 'Practice Information'. Below the header, there are instructions: 'Add your [practice information](#) to your security risk assessment. Consider all contexts of your organization's operations, such as various location(s), department(s), people, and more. Select '+ another location' if you have more than one location.' The form fields are: Practice Name (ABC Inc.), Address (123 Main St.), City, State, Zip (Ann Arbor, MI, 48105), Phone, Fax (800-888-8888, (xxx)-xxx-xxxx), Point of Contact (John Appleseed), Title/Role (Administrator), Phone (734-000-0000), and Email (John@abc.com). At the bottom right of the form are 'Delete' and 'Save this location' buttons. At the bottom of the page are '< Back' and 'Next >' buttons.

SRA Practice Information

practice assessment summary

Home Practice Info Assets Vendors Documents Assessment Reports Save Save As Logout

Add your [practice information](#) to your security risk assessment.
Consider all contexts of your organization's operations, such as various location(s), department(s), people, and more. Select '+ another location' if you have more than one location.

Practice Name: ABC Inc.

Address: 123 Main St.

City, State, Zip: Ann Arbor MI 48105

Phone, Fax: 800-888-8888 (xxx)-xxx-xxxx

Point of Contact: John Appleseed

Title/Role: Administrator

Phone: 734-000-0000

Email: John@abc.com

Delete Save this location

< Back Next >

The Practice Information screen captures some basic information from the practice(s) involved with the assessment.

This information will be included in the printable PDF report available once the assessment is completed.

Tracking Practice Assets



SRA Practice Assets

practice assessment summary

Enter your organization's [assets](#).
Consider all contexts of assets, such as your organization's location(s), department(s), equipment, people, materials, and more.
Want to [add more than one asset](#) at a time?

Add Asset Download Asset Template
 Export Asset List Upload Asset Template

Total Assets [3] Manage Multiple

Risk	Manage Assets		ID #	Type	Status	ePHI	Encryption	Assignment	Location
✓	Delete	Edit	129211	Laptop	Inactive [Stor...	Receives ePHI	File level encr...	John Applese...	Front Desk
✓	Delete	Edit	129233	Desktop	Not Disposed			Ryan	Hallway
✓	Delete	Edit	199229	Desktop	Active [In-use...	Receives ePHI	Full disk encr...	Wendy K	Office 2b

[Back](#) [Next](#)

The Assets screen captures a list of IT assets within a practice – computers, diagnostic/imaging equipment, network infrastructure, etc...

Assets can be entered one at a time, or imported in a list from a CSV file by using the Asset Template. **See video on next slide.**

Asset information can be exported from the SRA tool.

Practice Assets Continued



The screenshot displays the SRA Practice Assets interface. On the left is a blue sidebar with navigation links: Home, Practice Info, Assets, Vendors, Documents, Assessment, Reports, Save, Save As, and Logout. The main content area is titled 'Practice Assets' and includes instructions: 'Enter your organization's assets. Consider all contexts of assets, such as your organization's location(s), department(s), equipment, people, materials, and more. Want to [add more than one asset](#) at a time?'. An 'Add Asset' modal form is open, containing the following fields:

- Asset Type: Laptop
- Asset Status: Active [In-use and...]
- ePHI Access: Receives ePHI
- Disposal Status: Not applicable
- Disposal Date: (empty date field)
- Asset Encryption: Full disk encryption
- Asset Assignment: Cheryl
- Asset Location: Office 3a
- Asset ID: 129215
- Comments: (empty text area)


At the bottom of the modal is an 'Add' button. Below the modal, a table shows 'Total Assets [3]' with columns for Risk (all green) and Manage (all 'Delete' links). At the very bottom are '< Back' and 'Next >' buttons.

Available Fields

- Asset Type
- Asset Status – active, inactive
- ePHI Access – does it access PHI?
- Disposal Status – if inactive, has it been properly wiped/disposed?
- Disposal Date – date asset was disposed
- Asset Encryption – type of encryption protection of data
- Asset Assignment – who is responsible for this asset?
- Asset Location – physical location of the asset.
- Asset ID – asset tag or internal identifier
- Comments

Tracking Practice Vendors





Practice Vendors and Business Associates

practiceassessmentsummary

Home

Practice Info

Assets

Vendors

Documents

Assessment

Reports

Save


Save As


Logout


Enter your organization's [business associate & vendor information](#).


Consider all contexts of vendors & BAs, such as your organization's location(s), department(s), equipment, people, materials, and more.

Want to [add more than one vendor/BA](#) at a time?

Add Vendor or BA

Download Vendor/BA Template

Export Vendor/BA List

Upload Vendor/BA Template

Total Vendors/BAs [1]Manage Multiple

Manage Vendors		Vendor Name	Vendor Type	Satisfactory Assurances ...	Risks Assessed
Delete	Edit	Lab Testing LLC	Laboratory Services	Yes	Yes

< Back

Next >

The Practice Vendors screen captures a list of vendors, business associates, or third parties a practice may do business with.

Vendor information can be entered one at a time, or imported in a list from a CSV file using the Vendor Template.

Vendor information can also be exported from the tool.

Practice Vendors Continued



Add Vendor

Vendor Name: Lab Testing LLC

Service Type Provided: Laboratory Services

Vendor Address: 110 Fifth St.

City, State, Zip: Ann Arbor MI 48105

Phone, Fax: 800-000-0000 (xxx)-xxx-xxxx

Contact Name/Title: Roger A

Contact Email: roger@lservices.org

+ Second Contact

Have [satisfactory assurances](#) been obtained for this vendor? ☒ Yes ☐ No

Have additional risks been assessed for this vendor? ☒ Yes ☐ No

Add

< Back Next >

Available Fields

- Vendor Name
- Service Type Provided
- Vendor Address
- City, State, Zip
- Phone, Fax
- Contact Name/Title
- Contact Email
- Satisfactory Assurances – contract that PHI will be protected
- Additional Risks -
- + Second Contact – add another contact for the vendor

Practice Documentation



Documentation

practice

assessment

summary

Home

Practice Info

Assets

Vendors

Documents

Assessment

Reports

Save

Save As

Logout

Add [additional documentation](#) to your SRA.

Add documents, action item lists, references, remediation plans, or plan of action milestones relevant to your security risk assessment.

Add a Document

Manage Documents	Document Name	Section	Added By	Date Added
Delete	template_QA4.csv	N/A	Ryan	03-15-2022
Delete	detailed_pdf_QA5.pdf	N/A	Ryan	03-15-2022

< Back

Next >

The Documentation screen allows users to link to supporting documentation for the assessment.

No documents will be imported and saved into the tool, these are simply links to documents stored locally or on a local network to demonstrate accuracy and thoroughness of your responses.

Documents that have been added from the section summary screens (within the assessment) also display here.

Assessment



Section 5: Security and the Practice

practice

assessment

summary

Home

Practice Info

Assessment

Section 1 ✓

Section 2 ✓

Section 3 ✓

Section 4 ✓

Section 5

Section 6

Section 7

Reports

Save

Save As

Logout

Q3. Do you restrict physical access to and use of your equipment [i.e. equipment that house ePHI]?

☒ Yes. We have written policies and implemented procedures restricting access to equipment that house ePHI to authorized users only.

☐ Yes. We verbally authorize individuals to access equipment that house ePHI, but no written policies or procedures.

☐ No. We do not have a process to restrict access to equipment that house ePHI to authorized users.

☐ Flag this question for later.

Details:

The details field can be expanded to collect relevance and supporting information about the question/response.

Education

This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. Restrict access to assets with potentially high impact in the event of compromise. This

Reference

HIPAA: §164.310(a)(1)
NIST CSF: ID.RA, PR.AC, DE.CM, PR.IP
HICP: TV1, Practice # 6

< Back

Next >

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.

19

Rating Threats & Vulnerabilities



The screenshot displays the SRA (Security Risk Assessment) interface. The top navigation bar includes the SRA logo, the title 'Section 5: Security and the Practice', and tabs for 'practice', 'assessment', and 'summary'. The left sidebar contains navigation links: Home, Practice Info, Assessment, Section 1 through Section 7, Reports, Save, Save As, and Logout. The main content area is divided into two sections.

Vulnerability Selection Section: This section prompts the user to 'Select the vulnerabilities that apply to your practice from the list below.' It features a list of vulnerabilities with checkboxes:

- ☒ Inadequate facility access management procedures where information systems reside
- ☐ Inadequate physical protection for information systems
- ☐ Undocumented location of equipment or assets
- ☒ Inadequate access controls for business associate and vendor access
- ☒ Inadequate sanitation of media
- ☐ Inadequate procedures for proper workstation and connected network device security
- ☐ Failure to ensure user accounts are configured with appropriate permissions

Threat Rating Section: This section prompts the user to 'Please rate the likelihood and impact on your practice of each potential threat.' It displays a list of threats with Likelihood and Impact rating scales (L, M, H).

Threat	Likelihood	Impact
Unauthorized access to facility occurs undetected	L (green), M (grey), H (grey)	L (grey), M (yellow), H (grey)
Workforce and visitors access critical or sensitive business areas without authorization	L (grey), M (yellow), H (grey)	L (grey), M (grey), H (red)
Increased response time to respond to facility security incidents	L (grey), M (yellow), H (grey)	L (grey), M (yellow), H (grey)
Inconsistency in granting access to facilities	L (green), M (grey), H (grey)	L (green), M (grey), H (grey)
Inadequate access controls for business associate and vendor access	L (green), M (grey), H (grey)	L (grey), M (yellow), H (grey)
Adversary leverages third party access to gain access to facility and devices	L (green), M (grey), H (grey)	L (grey), M (yellow), H (grey)
Adversary leverages third party access to exfiltrate data or assets	L (grey), M (yellow), H (grey)	L (grey), M (grey), H (red)

At the bottom of the Threat Rating section, there are 'Back' and 'Next' buttons.

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.

Section Summary



Section 6: Complete!

Congratulations you've completed Section 6, on Security and Business Associates. Below is a summary highlighting where your practice is meeting the standard and potential areas of improvement.

78% 22%

Areas of Success

- Q1. Do you contract with business associates or other third-party vendors?
- Q2. Do you allow third-party vendors to access your information systems and/or ePHI?
- Q3. How do you identify which business associates need access to create, receive, maintain, or transmit ePHI?
- Q4. How does your practice enforce or monitor access for each of these

Areas for Review

- Q5. How do business associates communicate important changes in security practices, personnel, etc. to you?
- Q12. How does your practice document all of its business associates requiring access to ePHI?

Additional Information

Documents

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.

SRA Tool 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.

Flagged Report

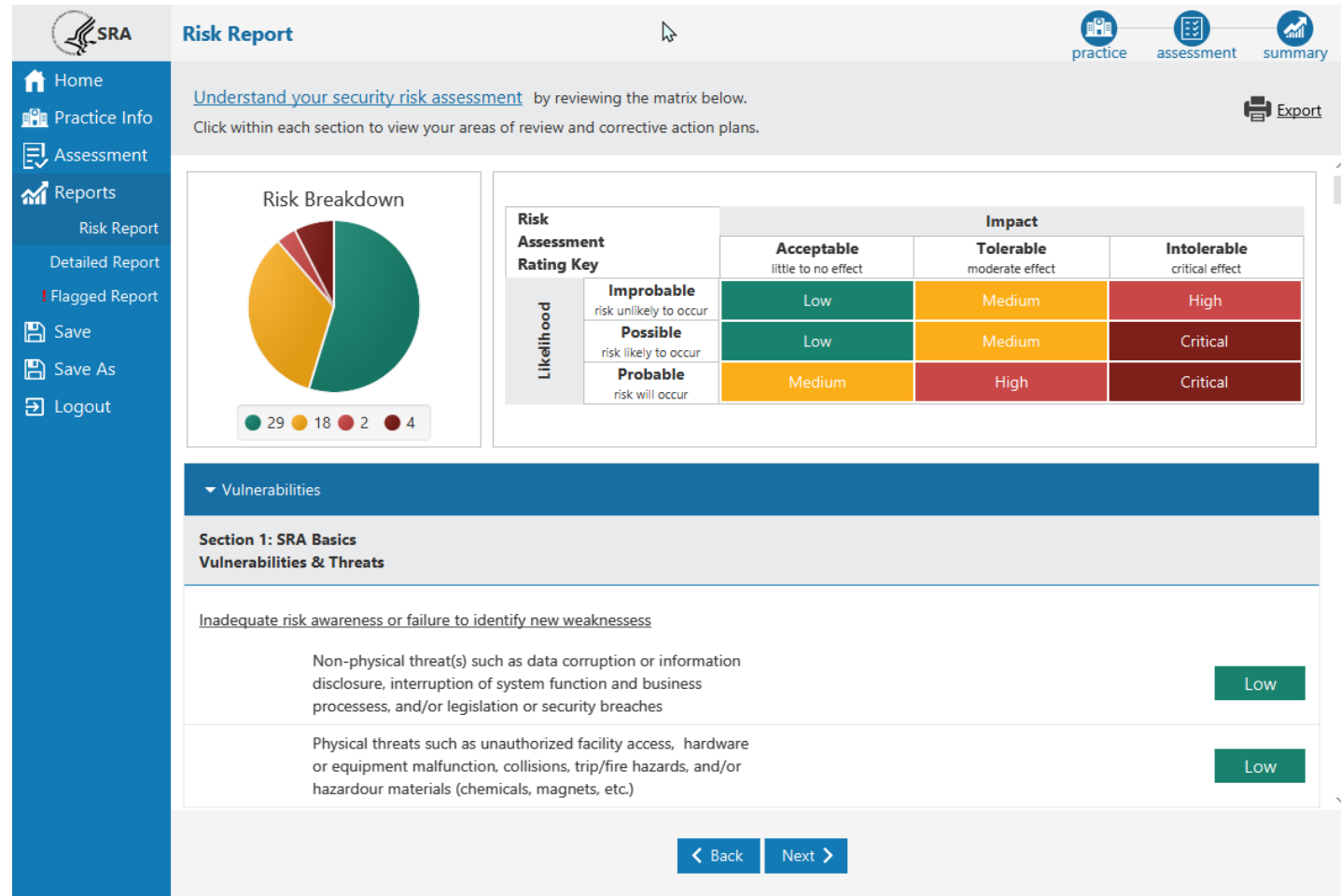


The screenshot shows the SRA (Security Risk Assessment) interface. On the left is a blue sidebar with navigation links: Home, Practice Info, Assessment, Reports (with sub-links for Risk Report, Detailed Report, and Flagged Report), Save, Save As, and Logout. The main header area includes the SRA logo, the title 'Flagged Report', and three icons for 'practice', 'assessment', and 'summary'. The main content area is titled 'Responses Flagged for Review:' and shows a 'count: 3'. Below this, a message states: 'To make changes to flagged questions, navigate back through the assessment using the Next/Back buttons.' The first section is '3 | Security & Workforce', containing question Q16: 'Do you ensure workforce members maintain ongoing awareness of security requirements?'. The answer is 'Flag this question for later.' Below the question are three radio button choices: 'Yes.', 'No.', and 'I don't know.' The second section is '4 | Security & Data', containing question Q21: 'Do you ensure users accessing ePHI are who they claim to be?'. The answer is also 'Flag this question for later.' with the same three radio button choices. At the bottom of the main content area is a blue button labeled '< Back'.

A report containing all of the questions you marked with “Flag this question for later.”

These questions should be reviewed and then answered more thoroughly.

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.

Detailed Report



Home

Practice Info

Assessment

Reports

Risk Report

Detailed Report

Flagged Report

Save

Save As

Logout

Detailed Report

Click each section to expand and review more details.

Infrastructure threat(s) such as building/road hazards, power/telephone outages, water leakage (pipes, roof, sprinkler activation), unstable building conditions

Low

Failure to meet minimum regulatory requirements and security standards

Corrective enforcement from regulatory agencies (e.g. HHS, OCR, FTC, CMS, State or Local jurisdictions)

Low

Damage to public reputation due to breach

Medium

Failure to attain incentives or optimize value-based reimbursement

Low

Litigation from breach victims due to lack of reasonable and appropriate safeguards

Low

Export Options

Question	Answer	Education	References	Compliance Guidance/Rule	Username	Date/Time
Q1. 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. Consider scheduling a vulnerability scan to improve your risk	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	Required	Ryan	Fri Mar 04 12:57:50 EST 2022

< Back

Next >

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.

Updating an SRA



Updating an Assessment

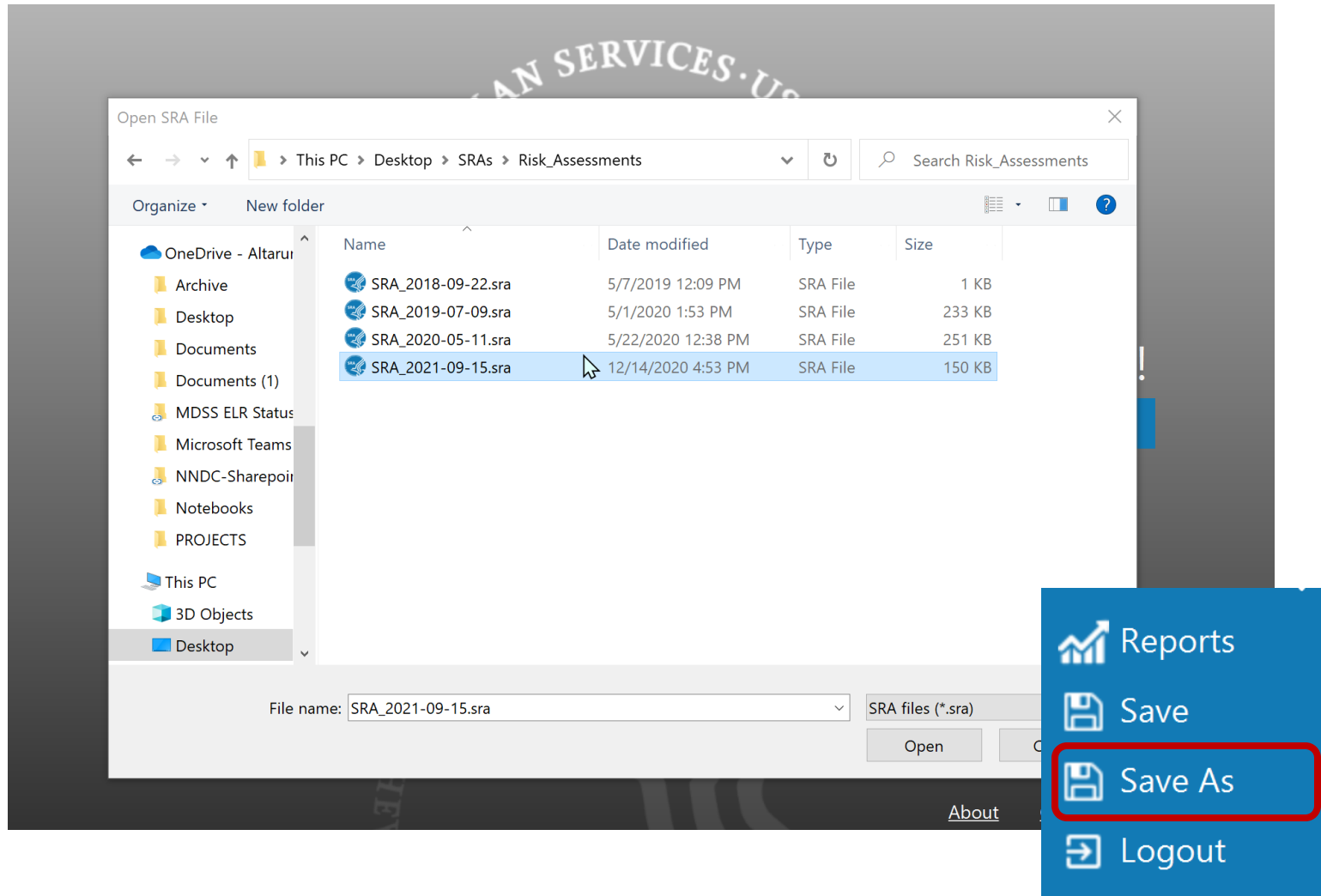


Considerations when reviewing an SRA instead of starting a new assessment:

- Length of time since your last assessment with the SRA Tool
- If there have been substantial changes in your organization
- Has the SRA Tool been updated recently?

Updates to the SRA Tool's content (questions, references, education) will only be applied when starting a NEW assessment


Updating an Assessment



Creating a new copy of an existing SRA file allows users to keep a historical record of assessments completed using the SRA Tool.

Updating an Assessment





Home

Practice Info

Assessment

Section 1 ✓

Section 2 ✓

Section 3 ✓

Section 4 ✓

Section 5 ✓

Section 6 ✓

Section 7 ✓

Reports

Save

Settings

Section 1: Complete!

Congratulations you've completed Section 1, on SRA Basics. Below is a practice is meeting the standard and potential areas of improvement.

< Jump to section start

57%

Areas of Success

Area

▶ Q1. Has your practice completed a security risk assessment (SRA) before?

▶

▶ Q4. Do you include all information systems containing processing and/or


▶

It is important to assess any changes to IT assets or vendor relationships in the Practice Information section




The “Jump to section start” button is a quick shortcut allowing the user to return to the first question in each section.

Updating an 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

Save

Save As

Logout

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 safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk assesment.

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 >

All questions should be reviewed thoroughly.

Use the Details field to record explanations or make note of changes

Complete review of all seven sections.

Updating an Assessment



- Start from the beginning of each section
- Read and re-evaluate each question
- Changing selections may result in a new path through assessment branching logic
- Utilize the details field to take notes as you go along

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*





New Enhancements

SRA Tool Version 3.3



Enhancements – Excel Workbook



Excel Workbook The SRA Tool is now available as an Excel Workbook in addition to the Windows Application.

This 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.

Section 1 - SRA Basics						
Question #	Question Text	Indicator	Question Responses	Guidance	Risk Indicated	Required? Reference
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
	NOTES:					
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
			Damage to public reputation due to breach	Medium	Medium	Medium

Enhancements – Excel Workbook



Section 1 - SRA Basics								
Question #	Question Text	Response Indicator	Question Responses	Guidance	Risk Indicated	Required?	Reference	
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. Consider scheduling a vulnerability scan to improve your risk assessment.		Required	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	
			No.	Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk assessment.		Required	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	
			I don't know.	Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI. Consider scheduling a vulnerability scan to improve your risk assessment.		Required	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	
			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 HICP: TV1, Practice # 7, 10	
	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. Document requirements to periodically update your risk assessment. You may also periodically conduct vulnerability scans.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI HICP: TV1, Practice # 10	
		✓	No.	Consider reviewing and updating your security risk assessment periodically. Document requirements to periodically update your risk assessment. You may also periodically conduct vulnerability scans.	Review	Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI HICP: TV1, Practice # 10	
			I don't know.	Consider reviewing and updating your security risk assessment periodically. Document requirements to periodically update your risk assessment. You may also periodically conduct vulnerability scans.		Required	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI HICP: TV1, Practice # 10	
			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 HICP: TV1, Practice # 10	
	Notes							
3	How often do you review and update your SRA?							
			Periodically and in response to operational changes and/or security incidents.	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,	

Enhancements – Excel Workbook



66	Threats & Vulnerabilities				Likelihood	Impact	Risk Score
67	1	Inadequate risk awareness or failure to identify new					
68			Non-physical threat(s) such as data corruption or		Low	Medium	Medium
69			Physical threats such as unauthorized facility		Low	Low	Low
70			Natural threat(s) such as damage from		Low	Low	Low
71			Man-Made threat(s) such as insider carelessness,		Medium	Medium	Medium
72			Infrastructure threat(s) such as building/road		High	High	Critical
73	2	Failure to remediate known risk(s)					
74			Information disclosure (ePHI, proprietary,		Low	Low	Low
75			Penalties from contractual non-compliance with		Low	Medium	Medium
76			Disruption of business processes, information		Medium	Medium	Medium
77			Data deletion or corruption of records		Low	High	High
78			Prolonged exposure to hacker, computer criminal,		Low	Low	Low
79			Corrective enforcement from regulatory agencies		Low	Low	Low
80			Hardware/equipment malfunction				
81	3	Failure to meet minimum regulatory requirements and security standards					
82			Corrective enforcement from regulatory agencies		Low	Low	Low
83			Damage to public reputation due to breach		Medium	Medium	Medium

Enhancements - HICP



Incorporating HICP We have incorporated references to Health Industry Cybersecurity Practices (HICP) into most questions within the tool. We have also enhanced the Education component with language from HICP.

HICP references are also shown inside reports and in the Excel Workbook.

The screenshot displays the 'Section 1: SRA Basics' interface. On the left is a blue sidebar with navigation links: Home, Practice Info, Assessment, Section 1 (selected), Section 2, Section 3, Section 4, Section 5, Section 6, Section 7, Summary, Save, Save As, and Logout. The main content area shows a question: 'Q4. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?'. Below the question are five radio button options: 'Yes.', 'No.' (selected), 'I don't know.', 'Other.', and 'Flag this question for later.'. To the right of the question area are two red-bordered boxes. The top box, titled 'Education', contains text about including ePHI in security risk assessments and maintaining an inventory of IT assets. The bottom box, titled 'Reference', lists references: 'HIPAA: N/A', 'NIST CSF: ID.RA, PR.DS', and 'HICP: TV1, Practice #5'. At the bottom of the interface are 'Back' and 'Next' buttons.

Section 1: SRA Basics

practice assessment summary

Q4. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?

☐ Yes.
☒ No.
☐ I don't know.
☐ Other.
☐ Flag this question for later.

Education

Include all information systems that contain, process, or transmit ePHI in your security risk assessment. In addition, document your systems in a complete inventory. Maintain a complete and accurate inventory of the IT assets in your organization to facilitate the implementation of optimal security controls. This inventory can be conducted and maintained using a well-designed spreadsheet.

Reference

HIPAA: N/A
NIST CSF: ID.RA, PR.DS
HICP: TV1, Practice #5

Details:

< Back Next >

Enhancements - HICP



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
Save
Save As
Logout

Q4. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?

☐ Yes.
☐ No.
☒ I don't know.
☐ Other.
☐ Flag this question for later.

Education

Include all information systems that contain, process, or transmit ePHI in your security risk assessment. In addition, document your systems in a complete inventory. Maintain a complete and accurate inventory of the IT assets in your organization to facilitate the implementation of optimal security controls. This inventory can be

Reference

HIPAA: N/A
NIST CSF: ID.RA, PR. DS, ID.AM
HICP: TV1, Practice # 5

Details:

< Back Next >

This question regarding IT asset management (ITAM) refers to HICP Technical Volume 1, Cybersecurity Practice #5

Enhancements - HICP



The screenshot shows the 'Security Risk Assessment' application window. The title bar says 'Security Risk Assessment'. The left sidebar has a blue header with 'SRA' and a home icon. Below it are links: Home, Practice Info, Assessment, Section 1, Section 2 ✓, Section 3 ✓, Section 4 ✓, Section 5 ✓, Section 6 ✓, Section 7 ✓, Reports, Save, Save As, and Logout. The main content area is titled 'Section 1: SRA Basics' and has tabs for 'practice', 'assessment', and 'summary'. A question 'Q4. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?' is displayed. Below the question are radio buttons for 'Yes', 'No', 'I don't know', 'Can't say', and 'False'. An informational popup is open over the question. The popup has a blue header 'Learn more...' and a blue body with the text 'HICP mitigate those threats. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes. HICP guidance seeks to cost-effectively reduce cybersecurity risks for small, medium, and large health care organizations and is consistent with HIPAA, NIST CSF, and HITECH provisions. The number corresponding to HICP in this frame refers to specific cybersecurity practices within the guidance that can be reviewed for more guidance around this question.' Below the text is a link 'HHS.gov - HICP Technical Volume 1' with a red arrow pointing to it. The popup also has a 'Reference' section with the following text: 'HIPAA: N/A', 'NIST CSF: ID.RA, PR. DS, ID.AM', and 'HICP: TV1, Practice # 5'. The popup has an 'Ok, got it!' button at the bottom. The main content area has a 'Details:' link at the bottom left and 'Back' and 'Next' buttons at the bottom center.

Clicking on the reference displays an informational popup about HICP and provides a link to HICP Technical Volume 1

Enhancements - HICP



Technical Volume 1: Cybersecurity | <https://405d.hhs.gov/Documents/tech-vol1-508.pdf>

17 of 29

Cybersecurity Practice #5: Asset Management

Organizations manage IT assets using processes referred to collectively as *IT asset management (ITAM)*. ITAM is critical to ensuring that the appropriate cyber hygiene controls are maintained across all assets in your organization.

ITAM processes should be implemented for all endpoints, servers, and networking equipment. ITAM processes enable organizations to understand their devices, and the best options to secure them. The practices described in this section may be used to support many of the practices described in other sections of this volume. Although it can be difficult to implement and sustain ITAM processes, such processes should be part of daily IT operations and encompass the lifecycle of each IT asset, including procurement, deployment, maintenance, and decommissioning (i.e., replacement or disposal) of the device.

Sub-Practices for Small Organizations

5.S.A	Inventory	NIST FRAMEWORK REF: ID.AM-1
-------	-----------	--------------------------------

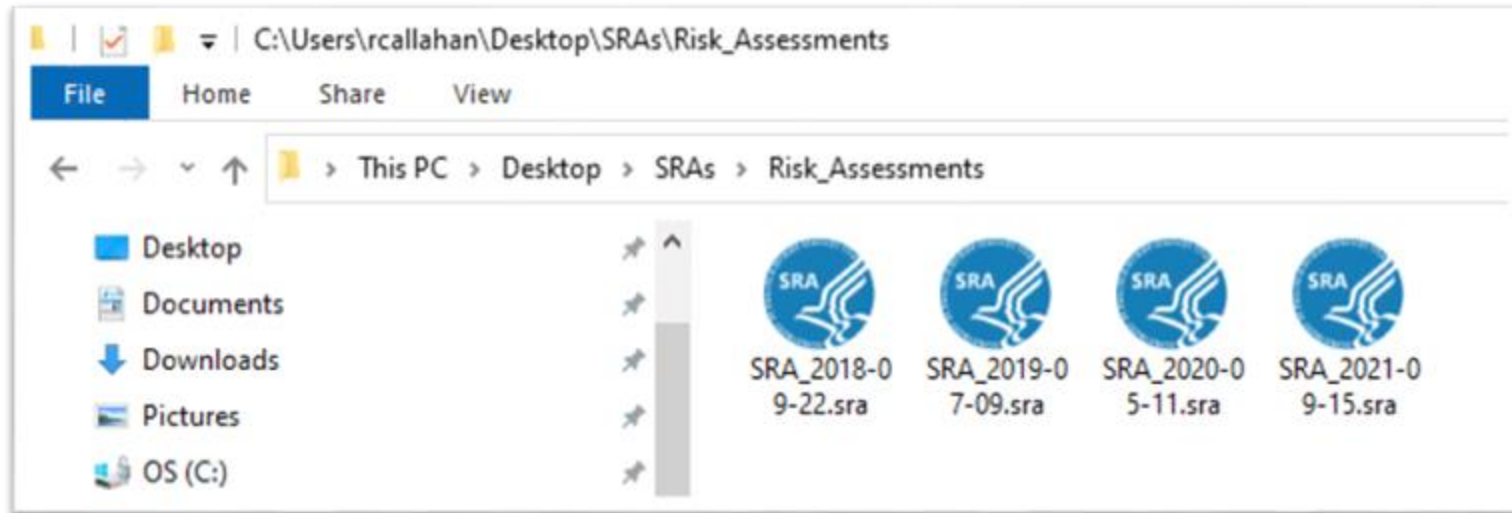
A complete and accurate inventory of the IT assets in your organization facilitates the implementation of optimal security controls. This inventory can be conducted and maintained using a well-designed spreadsheet. The following information should be captured for each device:

- Asset ID (primary key)
- Host Name
- Purchase Order
- Operating System
- Media Access Control (MAC) Address
- IP Address
- Deployed to (User)
- User Last Logged On
- Purchase Date
- Cost
- Physical Location

Remember to include all devices owned by your organization, including workstations, laptops, servers, portable drives, mobile devices, tablets, and smart phones.

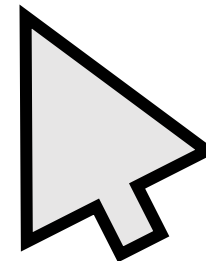
Cybersecurity Practice #5 gives the user more context about ITAM processes and which types of equipment should be considered.

Enhancements – File Association



SRA files can now be opened via the Windows file browser with a simple double-click.

Users no longer need to manually open the tool to work with their assessment.



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.

Question & Answer



Frequent Questions



- Where can I stay up to date with news about the SRA Tool?

OCR Listserv - <https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html>

ONC Email Updates – use “stay connected with ONC” on bottom of the page at HealthIT.gov

A blue rectangular box containing text and a form. The text is in yellow and white. The form consists of a white input field and a yellow button.

Stay connected with ONC
Subscribe to our Email Updates!

Please, enter your email address **Sign Up**

Frequent Questions



- Will the SRA Tool be made available for MacOS or iOS?
 - *Answer: Not at this time, but it's a frequent request so it may become a priority in the future. The SRA Tool Excel Workbook is a good option for MacOS users.*
- Does the tool support saving to network file share?
 - *Answer: Yes.*
- Can I import an SRA from v3.0 or 3.1 into v3.3 and beyond?
 - *Answer: Yes, anything created by version 3.0+ is compatible, but SRA's from v 2.0 are not compatible.*
- Once an SRA is complete, can you record mitigations inside the tool?
 - *Answer: Documents can be linked to your SRA. There are also notes fields present on each multiple-choice question and in each section summary. We also plan to have a space for notes in the spreadsheet version. Mitigations are not an explicit part of the SRA Tool application but are an important part of the risk assessment process and should be documented.*

Contact Us



Contact the SRA Tool Helpdesk:

Email: SRAHelpDesk@Altarum.org

Phone: 734-302-4717

Submit SRA Tool Questions via the [HealthIT Feedback Form](#)

Additional Information & Resources



- Visit [HealtIT.gov](https://www.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