

# SECURITY RISK ASSESSMENT TOOL | V3

Presenters: Lisa Steffey & Ryan Callahan  
Center for Connected Health | Altarum



The Office of the National Coordinator for  
Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

**OFFICE FOR CIVIL RIGHTS**



SOLUTIONS TO ADVANCE HEALTH

# Agenda



## Part one: SRA Tool Overview

- The Challenge and Solution
- SRA Tool Basics
- Tracking Vendors and Assets
- Completing the Assessment
- Understanding the Reports and Results

## Part two: Technical Assistance

- Questions & Answers
- Call for feedback

# Challenge

The healthcare industry faces constantly evolving cybersecurity threats and smaller healthcare providers often have limited time and resources to defend against the growing number of security risks.

The healthcare industry needs a Security Risk Assessment (SRA) tool that is easy to use and can help small practices evaluate their security posture against increasingly sophisticated security attacks.



# Solution

ONC engaged Altarum to design an improved version of the SRA Tool with a wizard-based workflow, updated layout, and an enhanced user experience that can assist users with their risk analysis process.

The new SRA Tool has over 56,645 downloads in the past year.

# Overview



The Security Risk Assessment (SRA) Tool guides users through security risk assessment process. It includes a self-paced modular workflow which includes a series of questions based on standards identified in the HIPAA Security Rule. Responses are sorted into [Areas of Success](#) and [Areas for Review](#).

The Guided Risk Framework walks users through an evaluation of potential Threats & Vulnerabilities so they can assess the likelihood and impact of threats to their practice. The SRA Tool may not address all risks that are known. Risks not addressed via the SRA Tool must be documented elsewhere.

Final Summary Reports are available once the user has completed the assessment process.

# Content



The SRA Tool's content was developed from 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

Upcoming content addition:

- Assessment questions will reference NIST Cybersecurity Framework guidance

# Assessment Content



Content within the Assessment is broken down into these main categories:

Section 1: Security Risk Assessment (SRA) Basics (security management process)

Section 2: Security Policies, Procedures, & Documentation (defining policies & procedures)

Section 3: Security & Your Workforce (defining/managing access to systems & workforce training)

Section 4: Security & Your Data (technical security procedures)

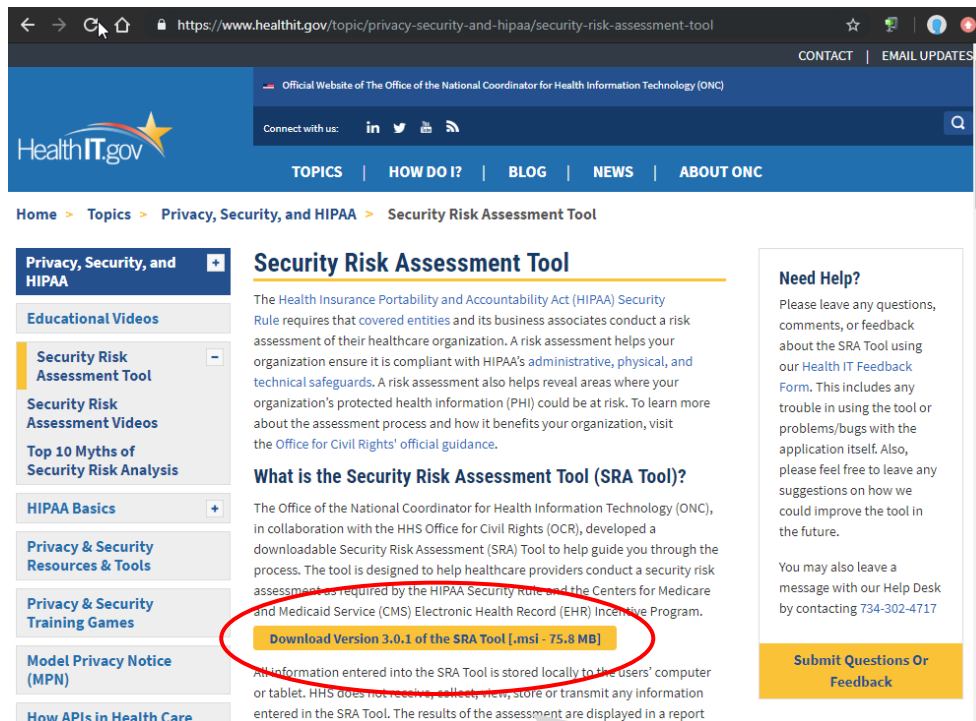
Section 5: Security & Your Practice (physical security procedures)

Section 6: Security & Your Vendors (business associate agreements and vendor access to PHI)

Section 7: Contingency Planning (backups and data recovery plans)

The tool offers dynamic content, so as the Security Rule and NIST guidelines evolve over time and new questionnaire content is developed, it can be downloaded and pulled into the SRA tool easily.

# Downloading and Installing the Tool



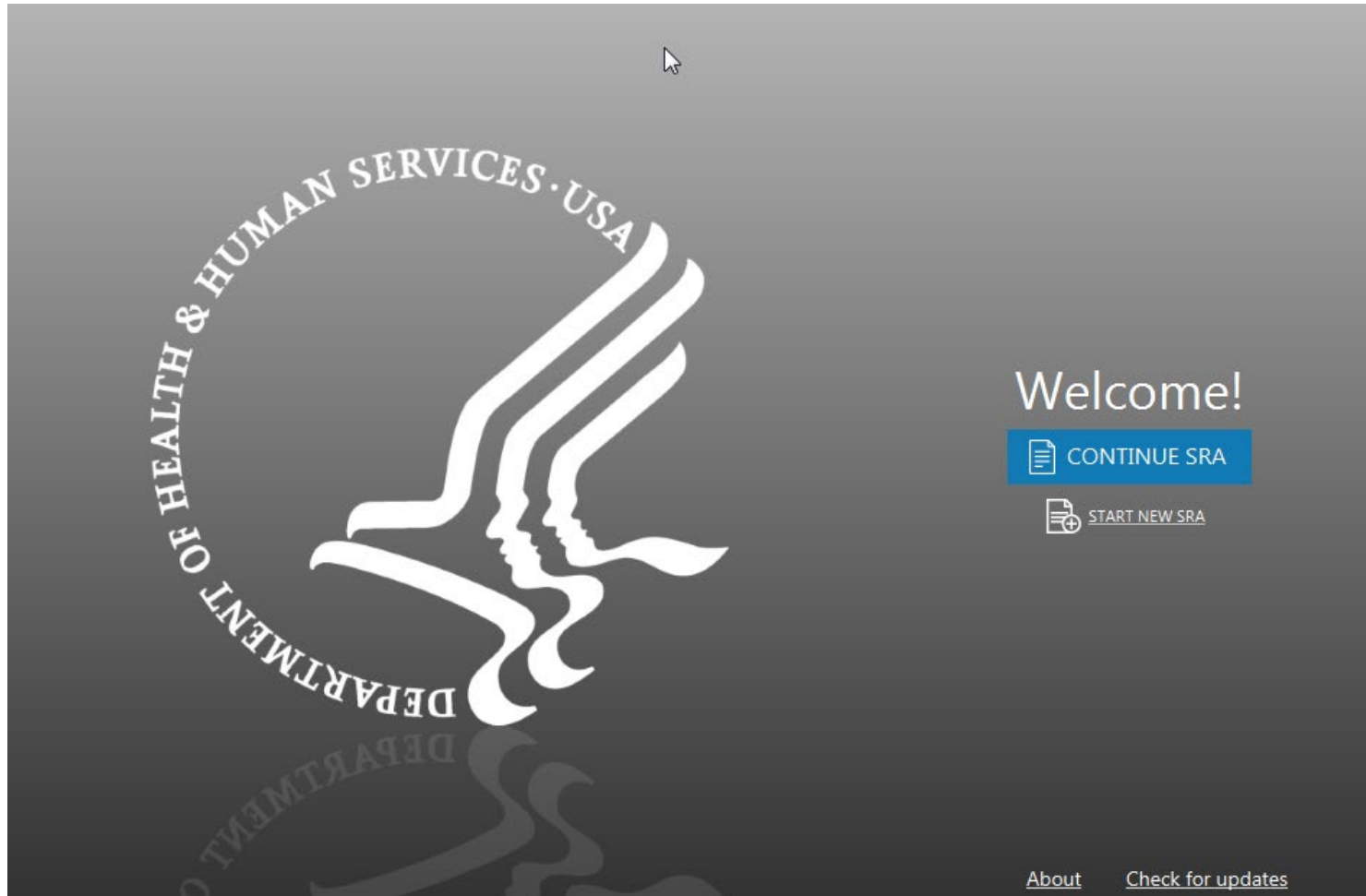
The tool can be downloaded from [HealthIT.gov](https://www.healthit.gov). The downloaded file is the installer for the tool. Double click to run the installer and walk through install process. Once downloaded, a blue “SRA-Tool” icon will appear on your desktop.

**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, and 10. All information entered into the tool is contained locally. No information is transmitted to DHHS, ONC or OCR.



# Welcome to the SRA Tool



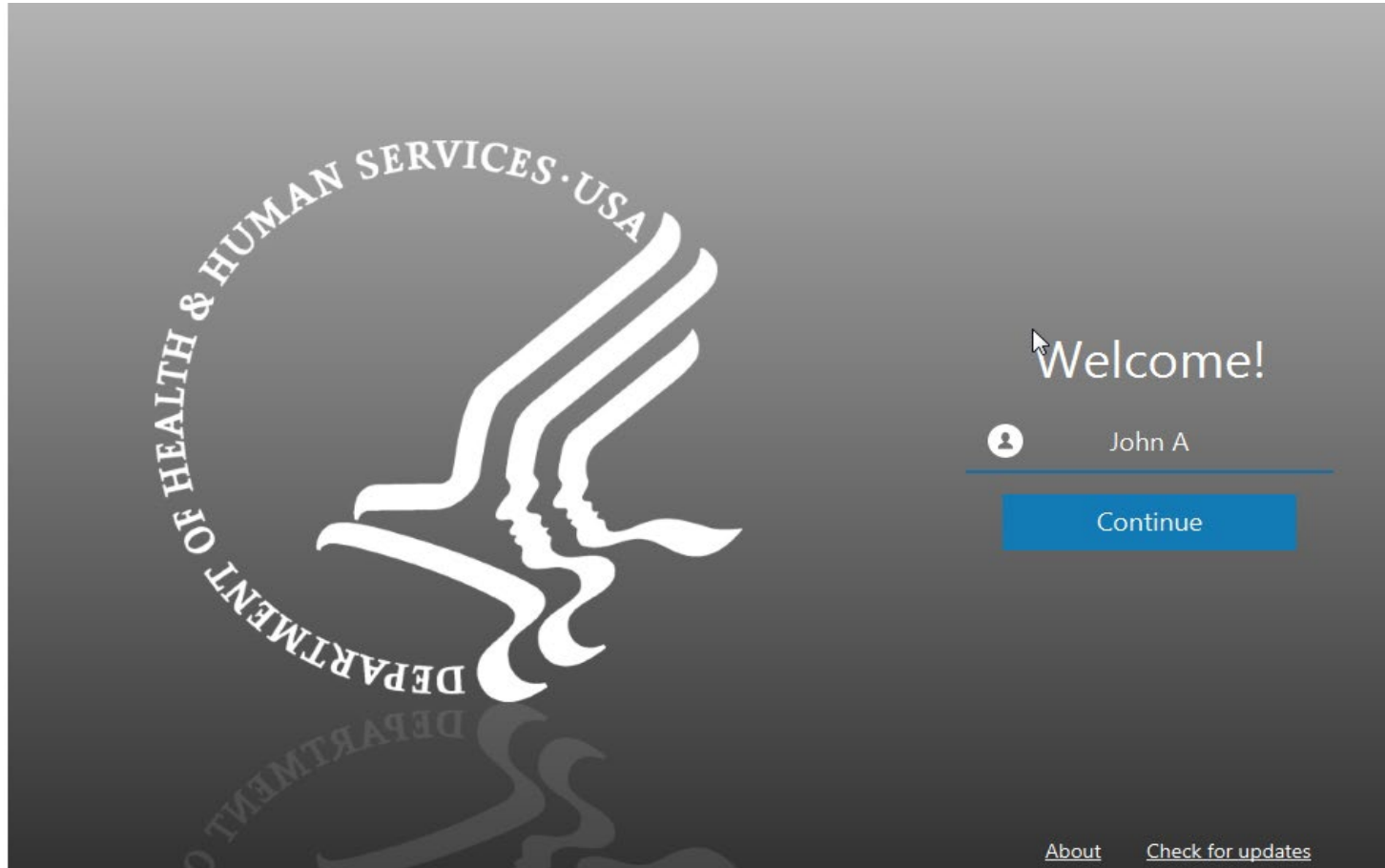
Select “Start New SRA” or “Continue SRA” to begin using the tool.

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.



# Entering a Username

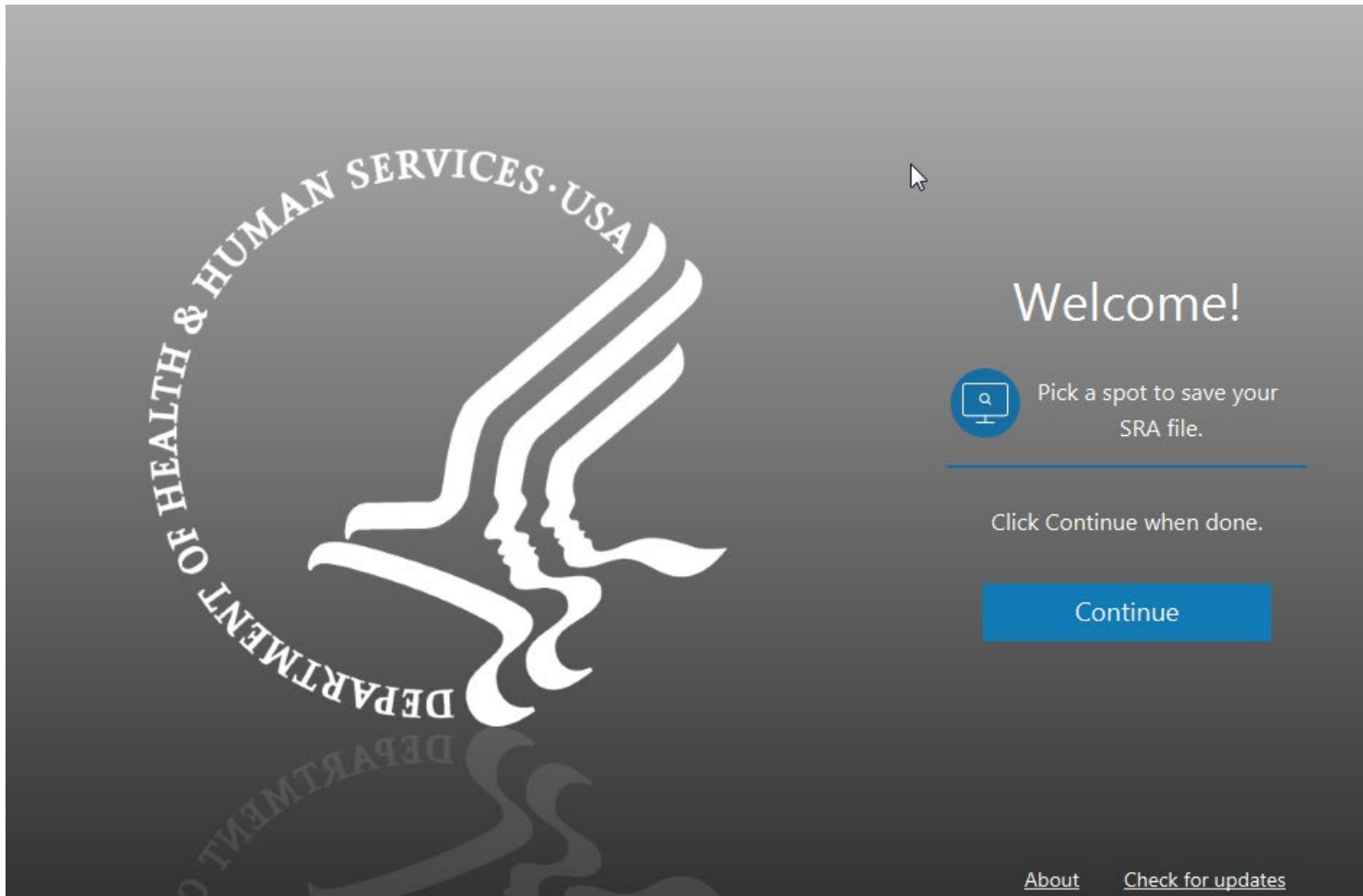


When beginning a new assessment, the user is asked to enter their name.

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



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



Security Risk Assessment

Home Practice Info Assessment Summary Save Logout

practice assessment summary

Welcome!

### What's a Security Risk Assessment?

A security risk analysis is the foundation upon which to build the security activities to protect ePHI. This tool will help you identify and assess the risks to ePHI in your practice so that you can implement appropriate safeguards.

**The SRA tool has 3 core steps:**

- Step 1:** Enter your practice information.
- Step 2:** Answer the assessment questions.
- Step 3:** Review your final risk report.

Next >

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' section of the SRA application. The left sidebar contains navigation links: Home, Practice Info, Assets, Vendors, Documents, Assessment, Summary, Save, and Logout. The main content area has a header with the SRA logo and 'Practice Information' title. Below the header are three icons: 'practice', 'assessment', and 'summary'. The main text reads: 'Add your [practice information](#) to your security risk assessment. Consider all contexts of your practice's operations, such as various location(s), department(s), people, and more. Select '+ another location' if you have more than one location.'

Practice Name	<input type="text" value="Family Health Center"/>
Address	<input type="text" value="123 N. Main St"/>
City, State, Zip	<input type="text" value="Ann Arbor"/> <input type="text" value="MI"/> <input type="text" value="48103"/>
Phone, Fax	<input type="text" value="734-000-0000"/> <input type="text" value="(xxx)-xxx-xxxx"/>
Point of Contact	<input type="text" value="Anne Smith"/>
Title/Role	<input type="text"/>
Phone	<input type="text" value="(xxx)-xxx-xxxx"/>
Email	<input type="text"/>

Buttons: Delete, Submit, + another location

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



**Practice Assets**

Enter your practice's [assets](#).

Consider all contexts of assets, such as your practice'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 [0]

Manage Assets	ID #	Type	Status	ePHI	Encryption	Assignment
No content in table						

< 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.

Asset information can be exported from the SRA tool.

# Practice Assets – Adding an Asset



## 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 ID – asset tag or internal identifier
- Comments

The screenshot shows the 'Add Asset' form in the SRA Practice Assets interface. The form is titled 'Add Asset' and has a close button (X) in the top right corner. The form contains the following fields:

- Asset Type:** A dropdown menu with 'Laptop' selected.
- Asset Status:** A dropdown menu with 'Inactive [Storage]' selected.
- ePHI Access:** A dropdown menu with 'Receives and tran...' selected.
- Disposal Status:** A dropdown menu with 'Not Disposed' selected.
- Disposal Date:** An empty text input field with a calendar icon.
- Asset Encryption:** A dropdown menu with 'Full disk encryption' selected.
- Asset Assignment:** A text input field containing 'John Appleseed'.
- Asset ID:** A text input field containing 'CID-22120'.
- Comments:** A large text area for entering comments.
- Add:** A blue button to submit the form.

At the bottom of the form, there are two buttons: '< Back' and 'Next >'. The background shows the SRA Practice Assets interface with a navigation menu on the left and a breadcrumb trail at the top: 'practice' > 'assessment' > 'summary'.

# Practice Assets – Adding Multiple Assets



**SRA Practice Assets**

practice assessment summary

Home: Enter your practice's [assets](#).

Practice Info: Consider all contexts of assets, such as your practice's location(s), department(s), equipment, people, materials, and more.

Assets: Want to [add more than one asset](#) at a time?

Vendors

Documents

Assessment

Summary

Save

Logout

Total Assets [0]

Manage Assets ID # Type Status ePHI Encryption Assignment



Add Asset



Download Asset Template



Export Asset List



Upload Asset Template

1

Step 1: Download the Asset Template from the SRA Tool Assets section.

3

Step 3: Upload your completed asset information .csv file into the SRA Tool.

2

Step 2: Enter your organization's asset information into the template (keeping the template format and the .csv file format)

Save the file once complete.

	A	B	C	D	E	F	G	H	I	J	K
1	Type	Assignment	ID	Asset Status	ePHI	Encryption	Comment	Disposal S	Disposal Date		
2	Desktop	Jane Smith	ID-221924	Active [In use	All of the	Full Disk		Not Disposed			
3	Desktop	Edward Randolph	ID-221925	Active [In use	All of the	Full Disk		Not Disposed			
4	Desktop	Hillary Belmont	ID-221926	Active [In use	All of the	Full Disk		Not Disposed			
5	Laptop	Jerry Lucas	ID-221927	Active [In use	All of the	Full Disk		Not Disposed			
6	Laptop	Jane Smith	ID-221928	Active [In use	All of the	Full Disk		Not Disposed			
7	Laptop	Edward Randolph	ID-221929	Active [In use	All of the	Full Disk		Not Disposed			
8	Laptop	Sally Waldo	ID-221930	Active [In use	All of the	Full Disk		Not Disposed			
9	Tablet	Jerry Lucas	ID-221931	Active [In use	All of the	Full Disk		Not Disposed			
10	Tablet	Edward Randolph	ID-221932	Active [In use	All of the	Full Disk		Not Disposed			
11	Phone	Jane Smith	ID-221933	Active [In use	Receives a	Full Disk		Not Disposed			
12	Phone	Edward Randolph	ID-221934	Active [In use	Receives a	Full Disk		Not Disposed			
13											
14											
15											

asset\_template

# Tracking Practice Vendors



**Practice Vendors**

practice assessment summary

Home Enter your practice's [business associates & vendor information](#).

Practice Info Consider all contexts of vendors, such as your practice's location(s), department(s), equipment, people, materials, and more.

Assets

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

Documents

Assessment

Summary

Save

Logout

Add Vendor or BAA

Download Vendor Template

Export Vendor List

Upload Vendor Template

Total Vendors [0]

Manage Vendors	Vendor Name	Vendor Type	Satisfactory Assura...	Risks Assessed
No content in table				

< 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 – Adding Vendor Info



**Add Vendor**

Vendor Name: Lab Testing Ilc.

Service Type Provided: laboratory services

Vendor Address: 110 Fifth St.

City, State, Zip: Ann Arbor MI 48103

Phone, Fax: (xxx)-xxx-xxxx (xxx)-xxx-xxxx

Contact Name/Title:

Contact Email:

+ Second Contact

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

Have additional risks been assessed for this vendor?  Yes  No

Add

## 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 Assessed
- + Second Contact – add another contact for the vendor

# Practice Documentation



**Documentation**

practice assessment summary

Home  
Practice Info  
Assets  
Vendors  
Documents  
Assessment  
Summary  
Save  
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
No content in table				

< 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



The screenshot displays the SRA Assessment interface. On the left is a blue navigation sidebar with icons and text for Home, Practice Info, Assessment, Section 1 (checked), Section 2, Section 3, Section 4, Section 5, Section 6, Section 7, Summary, Save, and Logout. The main content area is titled 'Section 2: Security Policies' and contains a question: 'Do you maintain documentation of policies and procedures regarding risk assessment, risk management and information security activities?'. Below the question are three radio button options. At the bottom of the main area are 'Back' and 'Next' buttons. On the right side, there are two red-bordered panels: 'Education' with text about documenting policies and procedures, and 'Reference' with text about Security Rule 45 CFR §164.316(a). At the top right of the main area are three circular icons labeled 'practice', 'assessment', and 'summary'.

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.

# Rating Threats & Vulnerabilities



The screenshot displays the SRA (Security Risk Assessment) interface. The top navigation bar includes 'practice', 'assessment', and 'summary' icons. The left sidebar contains navigation options: Home, Practice Info, Assessment, Section 1-7, Summary, Save, and Logout. The main content area is divided into two sections:

**Section 1: SRA Basics**  
Select the [vulnerabilities](#) that apply to your practice from the list below.

- Inadequate risk awareness or failure to identify new weaknesses
- Failure to remediate known risk(s)
- Failure to meet minimum regulatory requirements and security standards
- Inadequate Asset Tracking
- Unspecified workforce security responsibilities

**Section 1: SRA Basics**  
Please rate the likelihood and impact on your practice of each potential [threat](#).

	Likelihood			Impact		
<input checked="" type="checkbox"/> 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	L	M	H	L	M	H
Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardous materials (chemicals, magnets, etc.)	L	M	H	L	M	H
Natural threat(s) such as damage from dust/particulates, extreme temperatures, severe weather events, and/or destruction from animals/insects	L	M	H	L	M	H
Man-Made threat(s) such as insider carelessness, theft/vandalism, terrorism/civil unrest, toxic emissions, or hackers/computer criminals	L	M	H	L	M	H
Infrastructure threat(s) such as building/road hazards, power/telephone outages, water leakage (pipes, roof,	L	M	H	L	M	H

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.

# Assessment Section Review



The screenshot displays the SRA assessment interface. At the top, it says "Section 1: Complete!". Below this, a progress bar shows 89% completion in blue and 11% remaining in red. The interface is divided into two main columns: "Areas of Success" and "Areas for Review".

**Areas of Success:**

- Q1. Has your practice completed a security risk assessment (SRA) before?
- Q2. Do you review and update your SRA?
- Q3. How often do you review and update your SRA?
- Q6. What do you include in your SRA documentation?

**Your Answer:** Our SRA documentation includes possible threats and vulnerabilities which we assign impact and likelihood ratings to. This allows us to determine severity as needed.

**Additional Information**

**Areas for Review:**

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

**Your Answer:** No.

**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.

At the bottom right, there is a "Documents" button with a plus sign and a text input field.

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.

# Conducting a Thorough Assessment



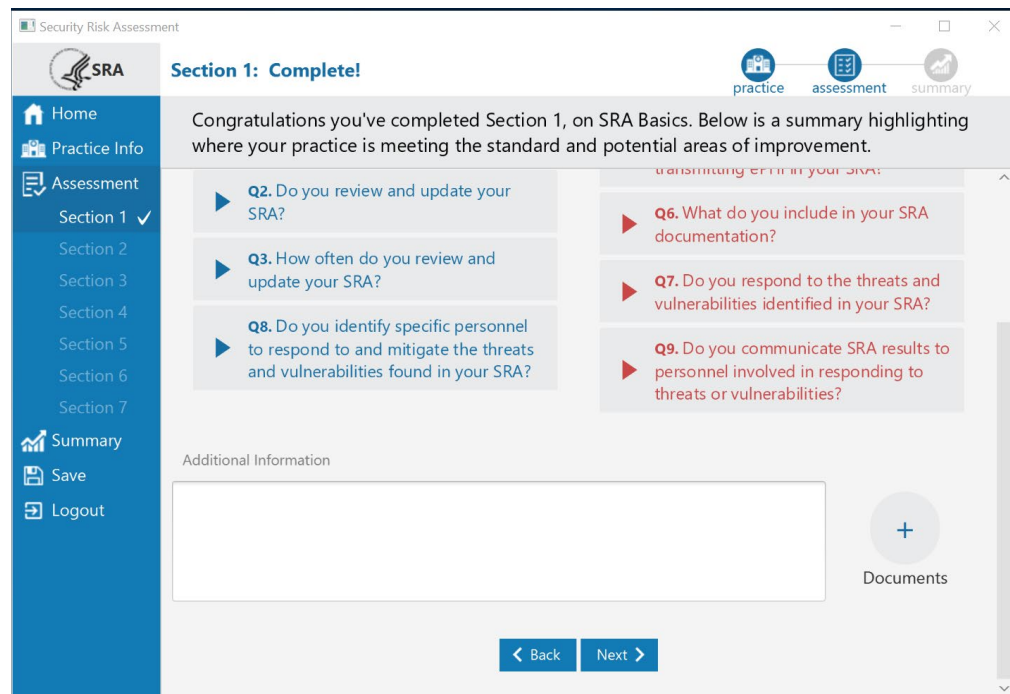
The HIPAA Security Rule's risk analysis requires an accurate and thorough assessment of the potential risks and vulnerabilities to all of the ePHI the organization creates, receives, maintains, or transmits.

- 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.

# Conducting a Thorough Assessment Continued

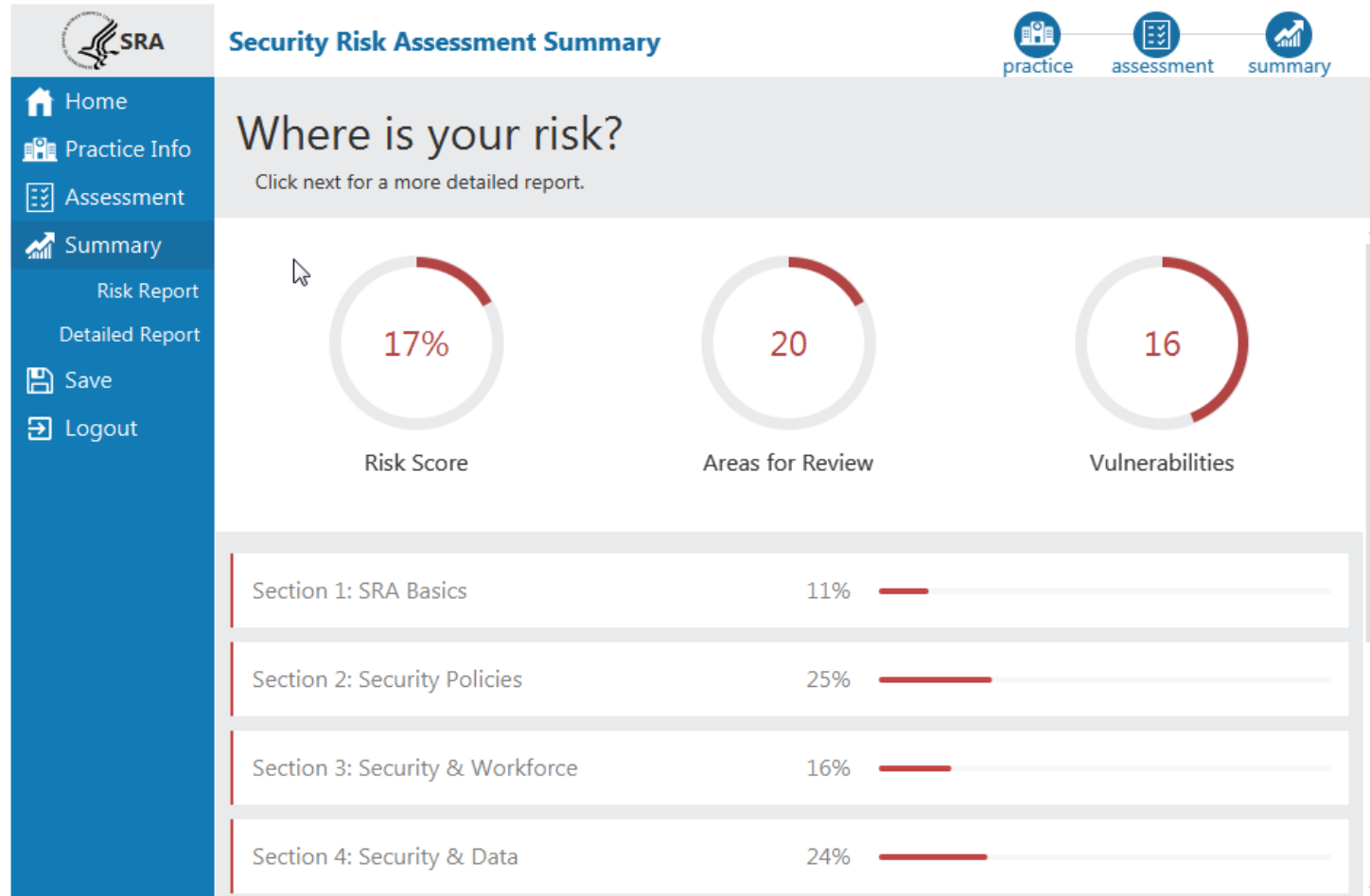


If potential risks to the confidentiality, integrity, and availability of an organization's ePHI are known to the organization, but unaccounted for by the SRA Tool, the organization should identify and assess these potential risks by either:



1. Documenting the potential risks in the most appropriate place within the tool.
2. Supplement the tool with additional documentation that includes the potential risks - supplemental documentation can be attached to the tool using the add document functionality.

# 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.

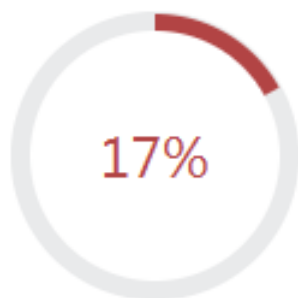
**Areas for Review** – shows the total number of questions answered sorted into Areas for Review.

**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.



# Understanding the Summary Report Scoring



Risk Score

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

The assessment section includes branching logic, so depending on how each user answers each question, they may be presented with different subsequent questions.



Areas for Review

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

This is a count across all assessment sections and provides the total number of questions in Areas for Review.



Vulnerabilities


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




This is a count across all assessment sections and provides to the total number of vulnerabilities the user selected as applicable to their organization.

The SRA Tool provides scoring in terms of Risk, not Compliance.

# Risk Report





**Risk Report**

 practice
  assessment
  summary

[Understand your security risk assessment](#) by reviewing the matrix below.  
Click within each section to view your areas of review and corrective action plans.

### Risk Breakdown



● 3
● 42
● 19
● 35

Risk Assessment Rating Key		Impact		
		Acceptable <small>little to no effect</small>	Tolerable <small>moderate effect</small>	Intolerable <small>critical effect</small>
Likelihood	<b>Improbable</b> <small>risk unlikely to occur</small>	Low	Medium	High
	<b>Possible</b> <small>risk likely to occur</small>	Low	Medium	Critical
	<b>Probable</b> <small>risk will occur</small>	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,

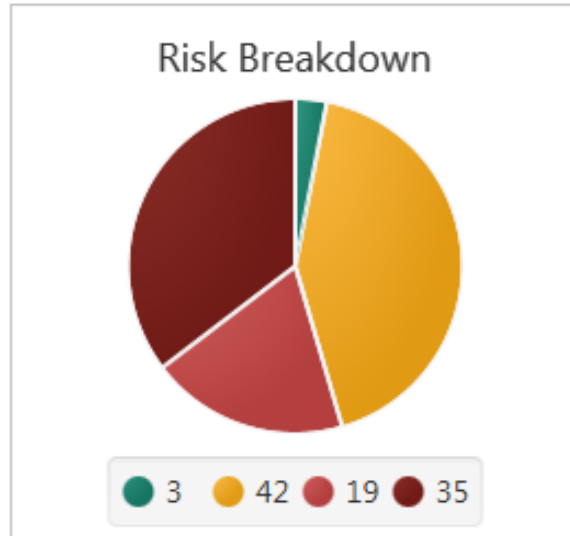
The Risk Report identifies all areas of risk collected across your entire assessment.

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.

# Understanding the Threats & Vulnerability Scoring



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


Threats & Vulnerabilities are categorized using a Risk Assessment Matrix as shown here. The Risk Breakdown pie chart shows a sum of threat ratings in each risk rating level (Low, Medium, High, and Critical).




During the assessment, each threat rated by the user in terms of likelihood and impact, is captured by the SRA Tool and provided risk rating level (Low, Medium, High, and Critical).

*For example, if a user selected a threat as having low likelihood, but high impact, the resulting risk level rating level would be High. The number of threats with a High risk rating level are then totaled and shown in the Risk Breakdown chart on the left.*

# Risk Report



**Risk Report**

    
practice assessment summary

[Understand your security risk assessment](#) by reviewing the matrix below.  
Click within each section to view your areas of review and corrective action plans.

▶ Vulnerabilities

▼ Areas for Review

Section	Question	Your Answer	Education
1	Q4. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?	No.	Include all information systems that contain, process, or transmit ePHI in your security risk assessment. In addition, document your systems in a complete inventory.
2	Q2. Do you review and update your security documentation, including	Yes, we review and update our documentation periodically or as needed	You should implement a process to periodically review and update your security policies and procedures. This will help

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



**SRA Detailed Report**

practice assessment summary

Click each section to expand and review more details.

▶ Section 1, SRA Basics Risk Score: 11%

▼ Section 2, Security Policies Risk Score: 25%

**Threats & Vulnerabilities** Risk Rating

Threat & Vulnerability	Risk Rating
<u>Failure to share security procedure information with appropriate parties</u>	
Unauthorized access to ePHI or sensitive information permitted	Medium
Disruption of information system function	High
ePHI exfiltrated to unauthorized entities	Medium
Insider carelessness causing disruption	Medium
Insider carelessness exposing ePHI	Critical

Question	Answer	Compliance Guidance/Rule	Username	Date/Time
Q1. Do you maintain documentation of policies and procedures regarding risk assessment, risk	Yes, we have a process by which management develops, implements, reviews, and updates	Required	Ryan	Wed Sep 26 09:53:47 EDT 2018

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.

The PDF button near the top right corner of the screen allows the user to save the Detailed Report as a PDF.

# Upcoming SRA Tool Enhancements



- Version 3.0.1 (current version)
  - Security updates
- 3.1 (upcoming release)
  - Highlight missed threat and vulnerability ratings
  - Mechanism to select multiple and “delete all” assets and vendors
  - Adding NIST Cybersecurity Framework references to each question
  - Excel export of Detailed Report
  - “In Process” reporting functionality, question flagging (skip question)

Follow @ONC\_HealthIT on Twitter to receive updates on the SRA Tool.

## Part Two: Call for User Feedback



- Submit feedback via the feedback form [here](#)
- Feedback can always be submitted to [SRAHelpDesk@Altatum.org](mailto:SRAHelpDesk@Altatum.org)

## Assistance with the SRA Tool



Reference the [SRA Tool User Guide](#) and additional information.

Contact the SRA Tool Helpdesk:

Email: [SRAHelpDesk@Altarum.org](mailto:SRAHelpDesk@Altarum.org)

Phone: 734-302-4717

Submit Questions through the [HealthIT Feedback Form](#)





ALTARUM.ORG