



Security Risk Assessment Tool

User Guide

DISCLAIMER

The Security Risk Assessment Tool at HealthIT.gov is provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with federal, state or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and professionals. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights (OCR) Health Information Privacy website at: www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

NOTE: The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool.

Create Date: October 16, 2018

Contents

Background	3
SRA Tool Overview	3
What to expect with the SRA tool	3
End User Hardware Requirements	5
Download Instructions	5
Using The Tool	5
Starting a New Assessment	5
Continuing an Assessment	6
Saving Assessment Progress	7
Add Practice Information	8
Add/Edit Asset Information	9
Upload Asset Template (Bulk Operations)	10
Add/Edit Vendor Information	12
Upload Vendor Template (Bulk Operations)	13
Completing the Assessment	14
Threat & Vulnerability Rating	15
Section Summary	16
Assessment Summary	17
Risk Report	18
Detailed Report	19
Saving & Exporting	20

BACKGROUND

Welcome to the Security Risk Assessment Tool 3.0 (SRA Tool), designed to help covered entities and business associates that handle patient information to identify and assess risks and vulnerabilities to the confidentiality, integrity, and availability of protected health information (PHI) in their environment. The HIPAA Security Rule requires health care providers, health plans and business associates to conduct risk analyses and implement technical, physical and administrative safeguards to protect Electronic Protected Health Information (ePHI). The Office for the National Coordinator for Health IT worked together with the Office for Civil Rights, which enforces the HIPAA Security Rule, to develop this tool to assist providers and business associates with meeting their responsibility to protect ePHI.

The tool is designed to help small to medium sized covered entities and business associates conduct and document risk assessments as part of their security management process, although healthcare providers of any size may use it. Through use of the SRA tool organizations can assess and document the information security risks to ePHI in their organizations.

We hope you find this tool helpful as you work towards improving the privacy protections and security of your organization and its compliance with the HIPAA Security Rule's risk analysis requirement. Please remember that this is only a tool to assist an organization with its review and documentation of its risk assessment, and therefore it is only as useful as the work that goes into performing and recording the risk assessment process. Once you have assessed your security risks using the tool, you may need to take appropriate steps to remediate any areas found wanting. Use of this tool does not mean that your organization is compliant with the HIPAA Security Rule or other federal, state or local laws and regulations. It does, however, help you comply with the HIPAA Security Rule requirement to conduct periodic security risk assessments.

SRA Tool Overview

Note: *The SRA Tool runs on your computer. It does not transmit information to the Department of Health and Human Services, The Office of the National Coordinator for Health IT, or The Office for Civil Rights.*

The SRA tool is hosted on ONC's website HealthIT.gov. It is a single downloadable module. The SRA tool is a Windows based application that can be installed locally on an end user's computer. With a wizard based workflow and section summary reporting, end users receive feedback and progress indicators as they work through the security risk assessment for their organization. It contains functionality to support multiple user accounts and a collaborative file sharing feature. In addition it allows organizations to track assets, current encryption levels for assets, business associates, and associated satisfactory assurances or risks pertaining those businesses. All user entered data is saved locally in a secure format (only accessible for decryption by the SRA tool).

The SRA Tool is a software application available for download from the ONC's HealthIT.gov website. It is available at no cost and can be used with Windows 7/8/9/10 operating systems. Legacy (SRA Tool 2.0) versions are also available for download. The legacy iOS SRA Tool application for iPad can be downloaded from the Apple App Store.

What to expect with the SRA tool

The SRA Tool guides covered entities and business associates through a series of questions based on the standards and implementation specifications identified in the HIPAA Security Rule and covers basic security practices, security failures, risk management, and personnel issues. There are currently 7 sections of content covering these areas:

- 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 and 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 sources of information used to support the development of the SRA Tool questionnaires include the following:

- HIPAA Security Rule
- National Institute of Standards and Technology (NIST) Special Publication 800-662
- NIST Special Publication 800-533
- NIST Special Publication 800-53A4
- Health Information Technology for Economic and Clinical Health (HITECH) Act

The SRA Tool takes you through each section by presenting a question about your organization's activities. Your answers will show you if you should take corrective action for that particular item or continue with your current security activities. If corrective action is suggested, the tool provides guidance on the related HIPAA Rule requirement or security reference and suggestions on how to improve. Following each assessment section, the tool prompts you to select applicable vulnerabilities and rate associated threats in terms of likelihood and impact to determine your risk level. The tool also provides section summaries with your results for each subset of questions.

The SRA Tool provides resources to help users...

- Understand the context of the question
- Consider the potential impacts to ePHI in your environment
- Identify relevant security references (e.g., the HIPAA Security Rule)

You can document your answers, comments, and risk remediation plans directly into the SRA Tool. **The tool serves as your local repository for the information.** Organizations can also attach supporting documentation of activities taken during the risk assessment process - for example, activities demonstrating how technical vulnerabilities are identified.

The HIPAA Security Rule's risk analysis requires an accurate and thorough assessment of the potential risks and vulnerabilities to all of an organization's ePHI, including ePHI on all forms of electronic media. If, after completing all of the questions in the SRA Tool, threats and vulnerabilities are known but are unaccounted for in the SRA Tool (i.e., a particular threat or vulnerability was not listed in the tool or the questions were not relevant to a risk area specific and known to the organization), the organization must either 1) document the unaccounted threats and vulnerabilities and assess the risks posed to ePHI in the most appropriate place within the SRA Tool, or 2) document the unaccounted threats and vulnerabilities and assess the risks posed to ePHI as part of a separate document to supplement the SRA Tool. Such documentation can be attached to the tool using the tool's the add document functionality.

Completing a risk assessment requires a time investment. At any time during the risk assessment process, you can pause to view your current results. The results are available in a color-coded graphic view and printable format.

Need Help? Please leave any questions, comments, or feedback about the SRA Tool using our Health IT Feedback Form. This includes any trouble in using the tool or problems/bugs with the application itself. Also, please feel free to leave any suggestions on how we could improve the tool in the future.*Persons using assistive technology may not be able to fully access information in this file. For assistance, contact ONC at PrivacyAndSecurity@hhs.gov.

End User Hardware Requirements

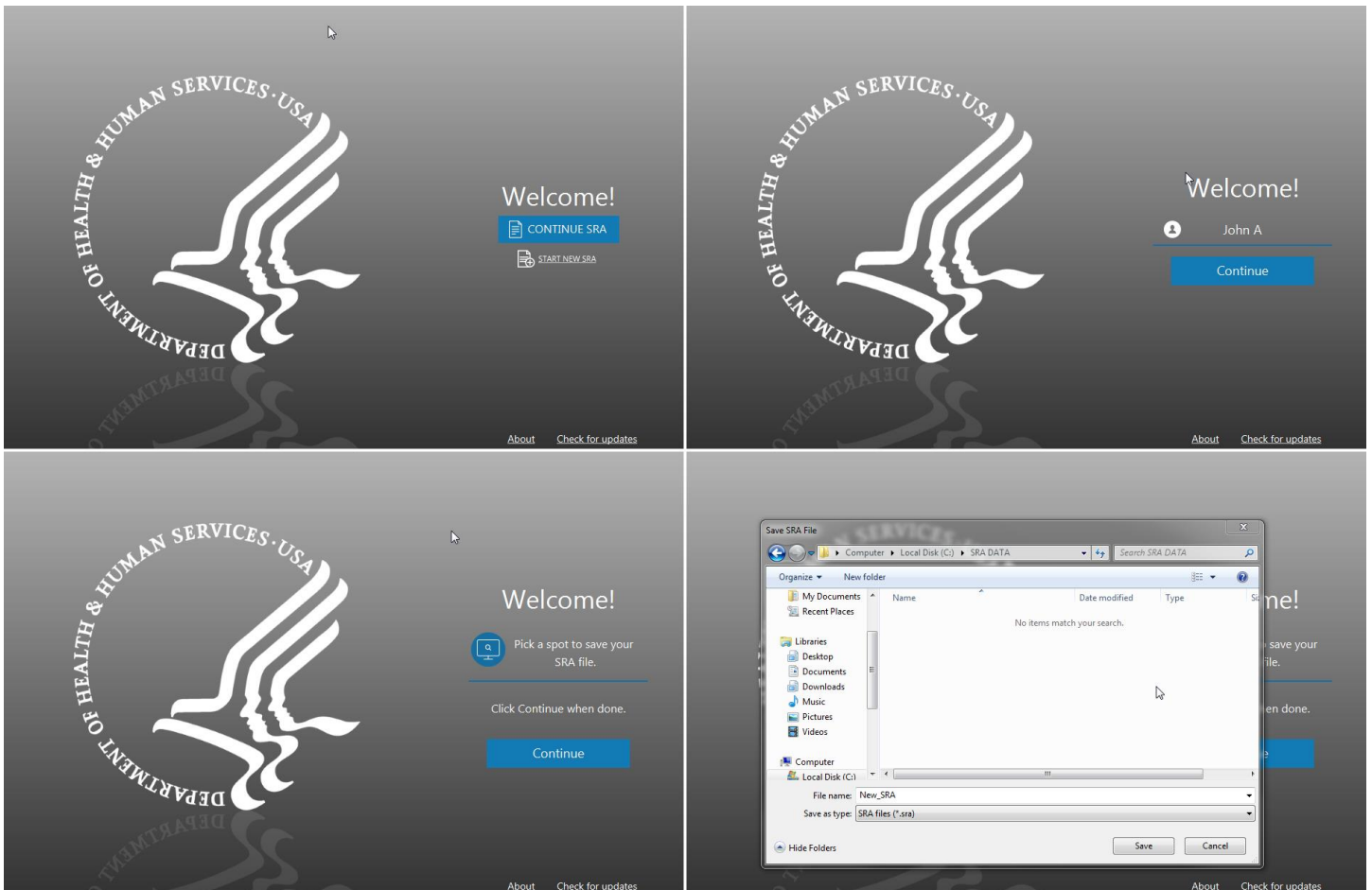
- Windows 7/8/10
- 2 GHz Pentium processor
- 2 GB RAM
- System type: 64-bit Operation System
- 1024 x768 screen resolution or better

Download Instructions

- Download the tool from the HealthIT.gov website
 - <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment>
- Once downloaded, run the downloaded executable to begin installation
- When installation is complete, double click on the SRA-Tool icon to begin

USING THE TOOL

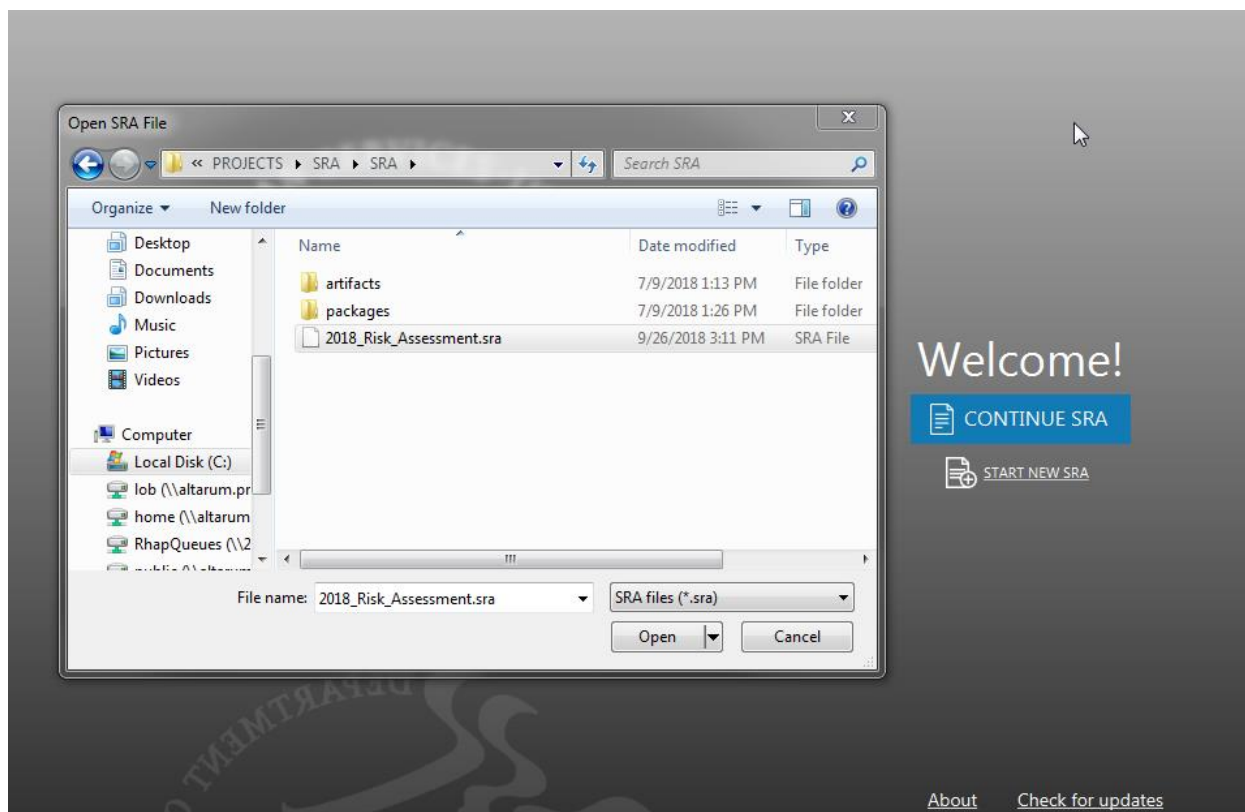
Starting a New Assessment



To start a new assessment, the SRA Tool must be downloaded and installed on a compatible system. The first steps to starting a new assessment are entering a user name of your choosing, creating a file name for your SRA, and selecting a location to save your SRA file.

1. Select "START NEW SRA".
2. Enter a user name. Click "Continue".
This can be simply a first name, first and last, initials, or anything else to distinguish the current user from any other parties intending to contribute to the risk assessment.
3. Select "Pick a spot to save your SRA file." This launches a system file browser.
In order to begin a new assessment and save progress, a location and file name for the .SRA file must be selected.
4. Choose a location and file name for the assessment, click "Save" when finished. Click "Continue" to move forward.

Continuing an Assessment



To continue an assessment that is in progress:

1. Launch SRA Tool.
2. Select "Continue SRA"
3. Navigate to location with saved .sra file (note that you cannot open SRA tool 2.0 files with SRA 3.0 except for bulk uploads of asset and vendor information)
4. Select the previously saved assessment and click "Open"
5. Select existing user or create new user.
6. Continue assessment.

Saving Assessment Progress

The screenshot displays the SRA tool interface for 'Section 7: Contingency Planning'. The top navigation bar includes 'practice', 'assessment', and 'summary' icons. The left sidebar menu shows 'Home', 'Practice Info', 'Assessment', 'Section 1-6' (all with checkmarks), 'Section 7' (highlighted), 'Summary', 'Save', and 'Logout'. The main content area features the question: 'How do you evaluate the effectiveness of your security safeguards, including physical safeguards?' with three radio button options:

- We have procedures in place to evaluate the effectiveness of our security policies and procedures, physical safeguards, and technical safeguards. Our evaluation is conducted periodically and in response to changes in the security environment.
- We have procedures in place to evaluate the effectiveness of our security policies and procedures, physical safeguards, and technical safeguards but we do not update them with any set frequency.
- We do not have a formal process to evaluate the effectiveness of our security safeguards.

At the bottom of the main content area are 'Back' and 'Next' buttons. The right sidebar contains two sections: 'Education' with the text 'This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.' and 'Standard' with the text 'Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes'.

Assessment progress can be saved at any time by clicking the Save button on the left navigation menu. Progress will be saved to the location the file was opened from.

Add Practice Information

The screenshot shows the 'Practice Information' form in the SRA Tool. The interface includes a blue sidebar with navigation options: Home, Practice Info (selected), 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, there 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.'

The form fields are as follows:

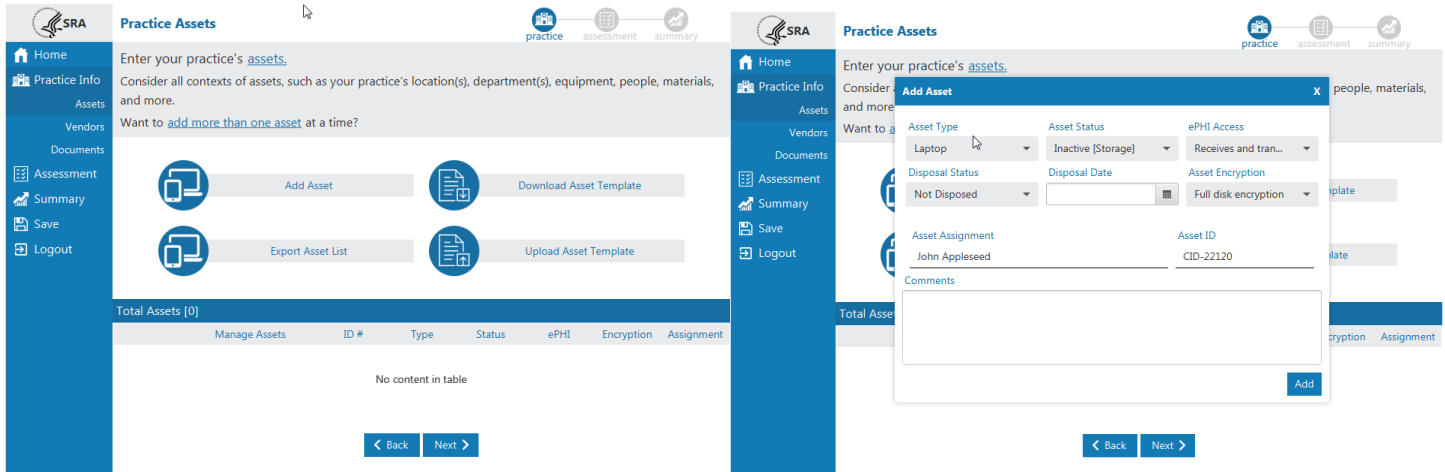
- Practice Name: Family Health Center
- Address: 123 N. Main St
- City, State, Zip: Ann Arbor, MI, 48103
- Phone, Fax: 734-000-0000, (xxx)-xxx-xxxx
- Point of Contact: Anne Smith
- Title/Role: (empty)
- Phone: (xxx)-xxx-xxxx
- Email: (empty)

Buttons: Delete, Submit, + another location

The SRA Tool provides a method to store practice information. Practice information is stored with assessment data and can be accessed by loading an SRA file and navigating to the Practice Info screen or by viewing the Detailed Report once the assessment is completed.

1. Enter information related to the practice. Select "**Submit**" after each practice information section is completed.
2. Multiple practice locations can be added by clicking "**+ another location**". After doing so, a new Practice Information section will appear. There is no limit on the amount of practices that can be added.
3. The "**Delete**" button can be used to remove any practice that is no longer needed. A prompt will appear directing the user to confirm the deletion of the selected practice.

Add/Edit Asset Information



The SRA Tool provides a method to track IT assets at a practice(s). Assets are stored with the assessment data and can be accessed by loading SRA file in the SRA Tool and viewing the Practice Assets screen or by viewing the Detailed Report after an assessment has been completed.

1. Select the **"Add Asset"** button from the Practice Assets Page. This page can be navigated to by pressing **"Next"** after Practice Info, or selecting **"Assets"** under the Practice Info item in the left navigation menu.
2. Enter information related to the asset:
 - a. **Asset Type**
 - b. **Asset Status** – is the asset currently in use?
 - c. **ePHI Access** – how does the asset interact with protected health information (PHI)
 - d. **Disposal Status** – If the device is no longer in use, was it disposed of?
 - e. **Disposal Date**
 - f. **Asset Encryption**
 - g. **Asset Assignment** – who, if anyone, is responsible for the asset?
 - h. **Asset ID** – any internal identification system used to uniquely identify the asset.
3. Select **"Add"** to add the asset. The asset will appear in the table at the bottom of the screen.
4. Selecting the **"X"** in the top right corner of the asset window will cancel the operation.
5. Previously entered asset information can be edited by selecting **"Edit"** next to an asset in the table at the bottom of the Practice Assets screen. The Edit Asset window will appear, and behave similarly to the Add Asset window. Selecting **"Update"** at the bottom of the window saves changes.
6. Assets can be deleted by selecting **"Delete"** next to a particular asset in the table in the bottom of the Practice Assets page.

Upload Asset Template (Bulk Operations)

The screenshot shows the 'Practice Assets' interface. On the left is a navigation menu with options: Home, Practice Info, Assets, Vendors, Documents, Assessment, Summary, Save, and Logout. The main content area has a header with 'Practice Assets' and navigation icons for 'practice', 'assessment', and 'summary'. Below the header, there are instructions: '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?'. There are four buttons: 'Add Asset', 'Download Asset Template', 'Export Asset List', and 'Upload Asset Template'. Below these is a table titled 'Total Assets [1]' with columns: Manage Assets, ID #, Type, Status, ePHI, Encryption, and Assignment. The table contains one row for an asset with ID 'CID-22120', Type 'Laptop', Status 'Inactive [St...', ePHI 'Receives a...', Encryption 'Full disk en...', and Assignment 'John Apple...'. At the bottom of the interface are 'Back' and 'Next' buttons.

Manage Assets	ID #	Type	Status	ePHI	Encryption	Assignment
Delete Edit	CID-22120	Laptop	Inactive [St...	Receives a...	Full disk en...	John Apple...

Type	Assignment	ID	Asset Status	ePHI	Encryption	Comment	Disposal Status	Disposal Date
Laptop	John Appleseed	CID-22120	Inactive [Storage]	Receives and transmits ePHI	Full disk encryption		Not Disposed	9/20/2018
Laptop		CID-22613	Active [In-use and Unassigned]	Receives ePHI	Full disk encryption		Not Disposed	9/20/2018
Desktop	Laura Jones	CID-22165	Active [In-use and Assigned]	Receives and transmits ePHI	Full disk encryption		Not Disposed	9/20/2018
Ultrasonography		CID-22145	Active [In-use and Unassigned]	Creates ePHI	File level encryption		Not Disposed	9/20/2018
Printer, Copier, Fax machine			Active [In-use and Assigned]	All of the above	No encryption		Not Disposed	9/20/2018

Assets can be added and exported from the SRA tool in bulk. To do this, the tool uses a strictly formatted CSV template. Assets are exported from, and imported to the tool following the template. A blank template file can be downloaded from the Practice Assets screen.

It is important to remember that in order to work with the SRA Tool, files must be kept in CSV format. **The tool does not accept .xls or .xlsx files. Ensure that files retain the .csv extension and file type.**

Once assets have been added to an SRA file using the SRA Tool, the entered assets can be exported to a CSV file.

1. Select **"Export Asset List"** from the Practice Assets screen.
2. Acknowledge the data security warning. It is important to remember that the exported asset list is stored in plain text, unencrypted. Do not leave this file where unauthorized personnel could gain access to it.
3. Select a location and file name for the asset list. Select **"Save"**.

A blank asset template can be downloaded from the tool if a user wishes to import all assets from a CSV file.

1. Select **"Download Asset Template"** from the Practice Assets screen.
2. Select a location and file name for the asset template. Select **"Save"**.

Correctly formatted asset files can be uploaded to the tool as an alternative to manual entry from the user interface.

1. Add properly formatted asset information to a CSV file that follows the template.
2. Ensure that the file is saved as a .csv

3. Select the **“Upload Asset Template”** button from the Practice Assets screen
4. Navigate to and select the saved CSV file. Select **“Open”**.
5. Imported assets will appear in the table at the bottom of the Practice Assets screen.

Add/Edit Vendor Information

The SRA Tool Provides a method to track Vendors or business associates. Vendor information stored with the assessment data and can be accessed by loading SRA file in the SRA Tool and viewing the Practice Vendors screen or by viewing the Detailed Report after an assessment has been completed.

1. Select the **"Add Vendor or BA"** button from the Practice Vendors Page. This page can be navigated to by pressing **"Next"** after Practice Assets, or selecting **"Vendors"** under the Practice Info item in the left navigation menu.
2. Enter information related to the Vendor:
 - a. **Vendor Name**
 - b. **Service Type Provided**
 - c. **Vendor Address**
 - d. **Phone, Fax**
 - e. **Contact Name/Title** – primary contact from vendor
 - i. **+Second Contact** – a second contact can be recorded for a particular vendor. Selecting the **"+Second Contact"** button loads two additional contact fields for title and email. Clicking the button again will collapse the additional fields.
 - f. **Contact Email**
 - g. **Satisfactory Assurances** – written agreement to safeguard protected health information.
 - h. **Risks Assessed**
3. Select **"Add"** to add the vendor. The vendor will appear in the table at the bottom of the screen.
4. Selecting the **"X"** in the top right corner of the add vendor window will cancel the operation.
5. Previously entered asset information can be edited by selecting **"Edit"** next to a vendor in the table at the bottom of the Practice Vendors screen. The Edit Vendor window will appear, and behave similarly to the Add Vendor window. Selecting **"Update"** at the bottom of the window saves changes.
6. Vendors can be deleted by selecting **"Delete"** next to a particular vendor in the table in the bottom of the Practice Vendors page.

Upload Vendor Template (Bulk Operations)

Practice Vendors

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

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

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

Buttons: 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 >

	A	B	C	D	E	F	G	H	I	J
1	Vendor Name	Service Type	Address	City	State	Zipcode	Phone	Fax	Contact N	Contact
2	Lab Testing Ilc.	laboratory services	111 Hoover Ave.	Ann Arbor	MI	48103	734-555-2222			
3	Cleaners	cleaning service	1909 Washtenaw Ave	Ann Arbor						
4										
5										
6										
7										
8										
9										

vendor_list

Vendor information can be added and exported from the SRA tool in bulk. To do this, the tool uses a strictly formatted CSV template. Vendors are exported from, and imported to the tool following the template. A blank template file can be downloaded from the Practice Vendors screen.

It is important to remember that in order to work with the SRA Tool, files must be kept in CSV format. **The tool does not accept .xls or .xlsx files. Ensure that files retain the .csv extension and file type.**

Once vendors have been added to an SRA file using the SRA Tool, the entered vendors can be exported to a CSV file.

1. Select **"Export Vendor List"** from the Practice Vendors screen.
2. Acknowledge the data security warning. It is important to remember that the exported vendor list is stored in plain text, unencrypted. Do not leave this file where unauthorized personnel could gain access to it.
3. Select a location and file name for the asset list. Select **"Save"**.

A blank vendor template can be downloaded from the tool if a user wishes to import all vendors from a CSV file.

1. Select **"Download Vendor Template"** from the Practice Vendors screen.
2. Select a location and file name for the vendor template. Select **"Save"**.

Correctly formatted vendor files can be uploaded to the tool as an alternative to manual entry from the user interface.

1. Add properly formatted vendor information to a CSV file that follows the template.
2. Ensure that the file is saved as a .csv
3. Select the **"Upload Vendor Template"** button from the Practice Vendors screen
4. Navigate to and select the saved CSV file. Select **"Open"**.
5. Imported assets will appear in the table at the bottom of the Practice Vendors screen.

Completing the Assessment

The screenshot displays the SRA tool interface for 'Section 1: SRA Basics'. The main content area asks, 'Has your practice completed a security risk assessment (SRA) before?'. Below this question are three radio button options: 'Yes.', 'No.', and 'I don't know.'. To the right of the question are two informational panels. The top panel, titled 'Education', states: 'Continuing to complete security risk assessments will help safeguard the confidentiality, integrity, and availability of ePHI.' The bottom panel, titled 'Standard', states: '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 held'. At the bottom of the screen are two buttons: 'Back' and 'Next'. The left sidebar contains navigation options: Home, Practice Info, Assessment, Section 1 (selected), Section 2, Section 3, Section 4, Section 5, Section 6, Section 7, Summary, Save, and Logout. The top navigation bar includes 'practice', 'assessment', and 'summary' tabs.

The assessment portion of the tool is broken down into sections. A list of sections can be seen on the left side of the screen while completing the assessment. The assessment contains branching logic that may serve questions in a different order depending on different response selections.

1. Each question in the assessment portion is single answer and multiple choice. This means that one answer and only one answer must be answered to continue.
2. The **Education** panel on the right side of the screen. When no answer is selected, the panel will be blank. Once a selection is made, information relevant to that selection will be displayed in the panel.
3. The **Reference** panel is on the right side of the screen. Reference to relevant security information regarding the question is shown here.
4. Selecting **"Next"** at the bottom of the screen progresses to the next question or section. After each multiple choice section, a threats and vulnerabilities rating section will be presented.

Threat & Vulnerability Rating

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
Summary
Save
Logout

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

< Back Next >

After completing each section of multiple choice questions, a set of vulnerabilities is presented. Multiple items can be selected. Select each vulnerability applicable to your practice.

1. Check the check box next to each applicable vulnerability.
2. Select "Next" to continue.

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
Summary
Save
Logout

Please rate the likelihood and impact on your practice of each potential [threat](#).

- Inadequate risk awareness or failure to identify new weaknesses

	Likelihood			Impact		
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

Each selected vulnerability has associated threats. Each threat must be rated based on the likelihood of occurrence at a practice, and the impact it would cause.

1. Make a selections for **"Likelihood"** and **"Impact"** for each threat listed.
 - a. L = Low
 - b. M = Medium
 - c. H = High
2. Both likelihood and impact for each threat must be rated before users can continue to the next screen.
3. Select **"Next"** to continue.

Section Summary

SRA Section 1: Complete!

practice assessment summary

Home
Practice Info
Assessment
Section 1 ✓
Section 2
Section 3
Section 4
Section 5
Section 6
Section 7
Summary
Save
Logout

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

89% 11%

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. We develop corrective action plans as needed to mitigate identified security

Areas for Review

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

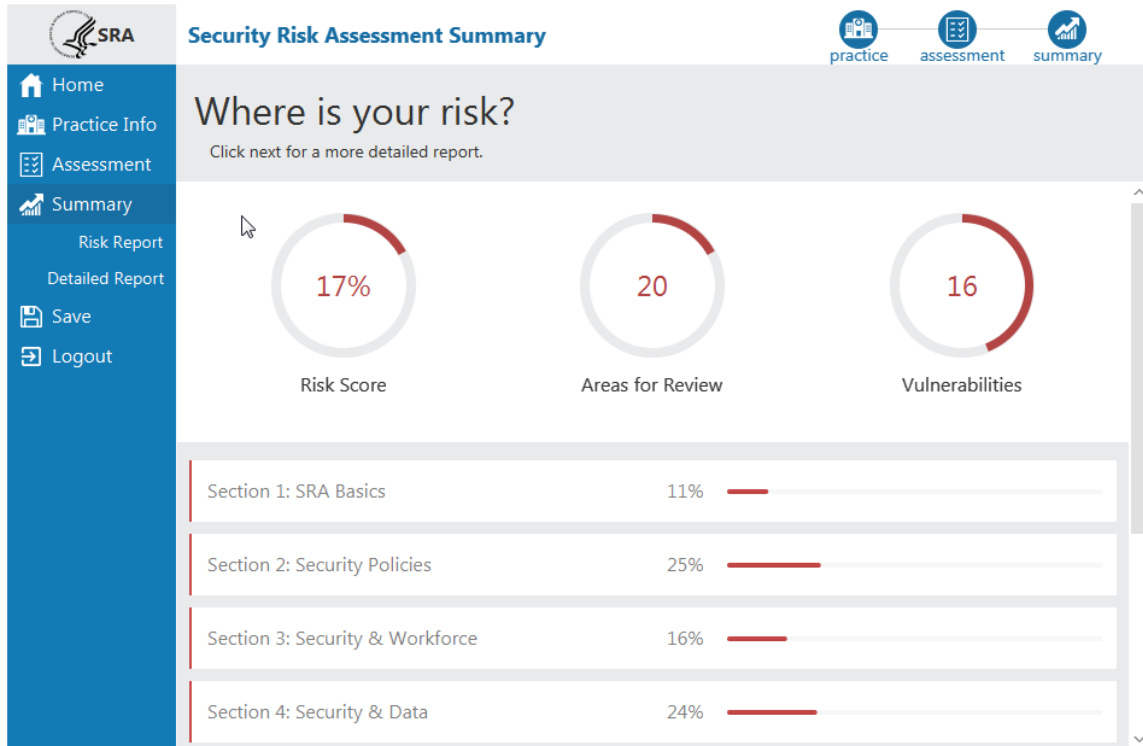
Your Answer: No.

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.

After completing multiple choice, threat selection, and vulnerability rating, a section summary is presented.

1. **Areas of Success** presents a list of questions where responses met the expectation, indicating compliance.
2. **Areas for Review** lists questions where responses indicated expectations are not being met, and review of process and procedures may be needed in order to improve safeguard efforts.
3. Clicking on the triangle on the left side of each question expands a tile revealing the chosen response and education information.
4. The graphic at the top of the screen represents the percentage of responses in the Areas of Success and Areas for Review categories respectively.

Assessment Summary



When all assessment sections have been completed, the SRA Summary screen is displayed. This screen shows percentages and visual representations of scores across all sections of the assessment.

1. **Risk Score** – percentage of responses sorted into Areas for Review across the whole assessment.
2. **Areas for Review** – count of responses sorted into the Areas for Review category.
3. **Vulnerabilities** – count of vulnerabilities selected as applicable to the practice.
4. **Section risk scores** – a percentage of responses sorted into Areas for Review for each section.

Risk Report

The Risk Report interface is divided into several sections:

- Risk Breakdown:** A pie chart showing the proportion of threats in each rating category. The counts are: 3 (Green), 42 (Yellow), 19 (Orange), and 35 (Red).
- Risk Assessment Rating Key:** A matrix combining Likelihood and Impact.
- Vulnerabilities:** A section listing vulnerabilities, currently collapsed.
- Areas for Review:** A table listing questions and responses, currently expanded.

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

Section	Question	Your Answer	Education
1	Q4. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRAT?	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 highlights responses from the multiple choice, threat, and vulnerability sections that indicate risk.

- Risk Breakdown** – This pie chart shows the proportion of threats in each rating category. The key below gives counts of threats in each category.
- Risk Assessment Rating Key** – This key shows how overall risk rating is calculated by combining threat likelihood with threat impact.
- Vulnerabilities** – All selected vulnerabilities are listed here along with their associated threats. Vulnerabilities are grouped by section
- Areas for Review** – All questions and responses sorted into Areas for Review are listed here along with education. Questions are grouped by section.
- Both Vulnerabilities and Areas for Review can be collapsed by clicking on the white triangle to the right of the respective headings.

Detailed Report

Detailed Report

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 Description	Risk Rating
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 an output of all the information entered into the SRA Tool, besides section comments and linked files. Each section is broken down into threats & vulnerabilities and multiple choice.

1. Each section is collapsible. Select the section title or black triangle to expand a section. Click again to collapse.
2. **Risk Score**, that is the percentage of multiple choice responses sorted into Areas for Review, is displayed for each section.
3. **Risk Rating** is a combination of likelihood and impact rating for each threat. The Risk Assessment Rating Key on the Risk Report shows how Risk Rating is calculated.
4. Practice Information, Asset Information, and Business Associates and Vendors are all displayed at the bottom of the Detailed Report.
5. The grey PDF icon at the top right corner of the report allows the Detailed Report to be saved as a PDF. Click the icon and select a name and location to save the PDF file.


Saving & Exporting

There are a few ways to save information entered into the SRA Tool:

- 1. Save Detailed Report as PDF**

The Detailed Report is a complete output of information captured by the tool minus section comments and linked documents. It contains Practice Information, Assets, Vendors, multiple choice, vulnerabilities, and threats.



The Detailed Report can be saved as a PDF by clicking the  icon near the top right corner of the report screen.

- 2. Export Asset List**

Asset information entered into the tool can be exported as a CSV file by selecting "**Export Asset List**" from the Asset Information screen. This is a useful method to move assets from one SRA file to another without re-entering each one individually.

- 3. Export Vendor List**

Vendor information entered into the tool can be exported as a CSV file by selecting "**Export Vendor List**" from the Vendor Information screen. This is a useful method to move vendor information from one SRA file to another without re-entering each one individually.