

The Security Risk Assessment Tool

Overview for Small and Medium Practices

Presenters: Ryan Callahan, Nick Heesters



**Office of the National Coordinator
for Health Information Technology**



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

Agenda

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

What is Security Risk Assessment?

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

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

HIPAA § 164.308(a)(1)(ii)(A)

Risk Analysis components of a Security Risk Assessment:

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

Outcomes from security risk assessment

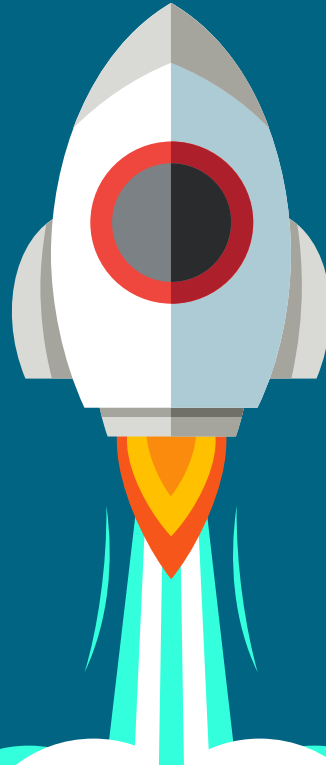
Organizations should use information gleaned from their assessment to implement security measures to:

- Design personnel screening processes
- Identify and strategize data backup
- Determine where and how encryption should be used
- Determine what authentication may be required to protect data integrity
- Determine which policies and procedures may need to be created or improved to protect ePHI



Challenge

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



SRA Tool

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

The SRA Tool

The screenshot displays the SRA Tool interface. At the top, the window title is "Risk Assessment". Below it, the page header shows "SRA" and "Section 1: SRA Basics". On the right side of the header, there are three icons: "practice", "assessment", and "summary".

A left-hand navigation menu is visible, listing the following items: Home, Practice Info, Assessment, Section 1, Section 2 ✓, Section 3 ✓, Section 4 ✓, Section 5 ✓, Section 6 ✓, Section 7 ✓, Reports, Glossary, Save, Save As, and Logout. At the bottom of this menu is a link for "Version Information".

The main content area features a question: "Q10. How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?". Below the question are five radio button options:

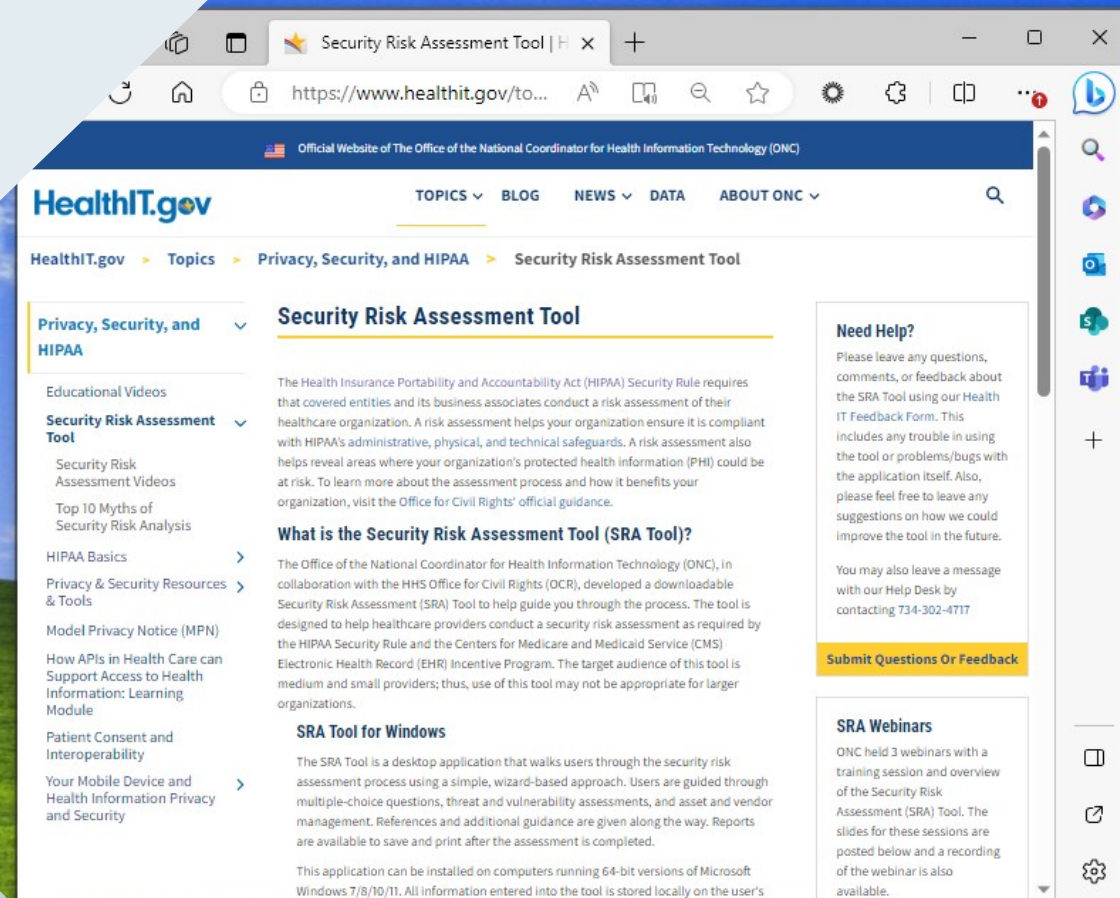
- Written and verbal communication as well as coordinated corrective action planning.
- Written communication only.
- Verbal communication only.
- We do not communicate risk assessment results to workforce members.
- Flag this question for later.

On the right side of the question area, there are two informational boxes:

- Education:** Written results of your SRA should be communicated to the personnel responsible for responding to identified threats and vulnerabilities but also consider involving the personnel responsible for responding to identified threats and vulnerabilities in the creation of corrective action plans.
- Reference:**
 - HIPAA:** §164.308(a)(1)(ii)(B)
 - NIST CSF:** ID.RA, ID.RM, RS.MI
 - HICP:** N/A

At the bottom of the question area, there is a "Details:" link. At the very bottom of the interface, there are two buttons: "< Back" and "Next >".

Downloading, Installing, and Using the SRA Tool



The screenshot shows a web browser window displaying the HealthIT.gov website. The browser's address bar shows the URL <https://www.healthit.gov/to...>. The website header includes the HealthIT.gov logo and navigation links for TOPICS, BLOG, NEWS, DATA, and ABOUT ONC. The main content area is titled "Security Risk Assessment Tool" and is part of the "Privacy, Security, and HIPAA" section. A left sidebar contains a list of related topics, with "Security Risk Assessment Tool" selected. The main text explains that the tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule. It also includes a section titled "What is the Security Risk Assessment Tool (SRA Tool)?" and a section for "SRA Tool for Windows". A right sidebar contains a "Need Help?" section with contact information and a "Submit Questions Or Feedback" button. The background of the website is a blue sky with white clouds.

Security Risk Assessment Tool | H x +

https://www.healthit.gov/to...

Official Website of The Office of the National Coordinator for Health Information Technology (ONC)

HealthIT.gov

TOPICS ▾ BLOG NEWS ▾ DATA ABOUT ONC ▾

HealthIT.gov > Topics > Privacy, Security, and HIPAA > Security Risk Assessment Tool

Privacy, Security, and HIPAA ▾

- Educational Videos
- Security Risk Assessment Tool**
- Security Risk Assessment Videos
- Top 10 Myths of Security Risk Analysis
- HIPAA Basics >
- Privacy & Security Resources & Tools >
- Model Privacy Notice (MPN)
- How APIs in Health Care can Support Access to Health Information: Learning Module
- Patient Consent and Interoperability
- Your Mobile Device and Health Information Privacy and Security >

Security Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. To learn more about the assessment process and how it benefits your organization, visit the [Office for Civil Rights' official guidance](#).

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

SRA Tool for Windows

The SRA Tool is a desktop application that walks users through the security risk assessment process using a simple, wizard-based approach. Users are guided through multiple-choice questions, threat and vulnerability assessments, and asset and vendor management. References and additional guidance are given along the way. Reports are available to save and print after the assessment is completed.

This application can be installed on computers running 64-bit versions of Microsoft Windows 7/8/10/11. All information entered into the tool is stored locally on the user's

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.

You may also leave a message with our Help Desk by contacting 734-302-4717

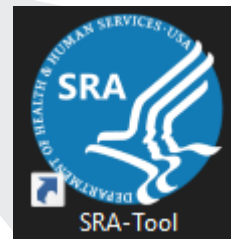
[Submit Questions Or Feedback](#)

SRA Webinars

ONC held 3 webinars with a training session and overview of the Security Risk Assessment (SRA) Tool. The slides for these sessions are posted below and a recording of the webinar is also available.

Download & Installation

The screenshot shows the HealthIT.gov website page for the Security Risk Assessment Tool. The URL is https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool. The page features a navigation menu with links for TOPICS, HOW DO I?, BLOG, NEWS, and ABOUT ONC. The main content area is titled "Security Risk Assessment Tool" and includes a description of the tool, a "What is the Security Risk Assessment Tool (SRA Tool)?" section, and a "Download Version 3.0.1 of the SRA Tool [.msi - 75.8 MB]" button circled in red. A "Need Help?" section is also visible on the right side of the page.



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.

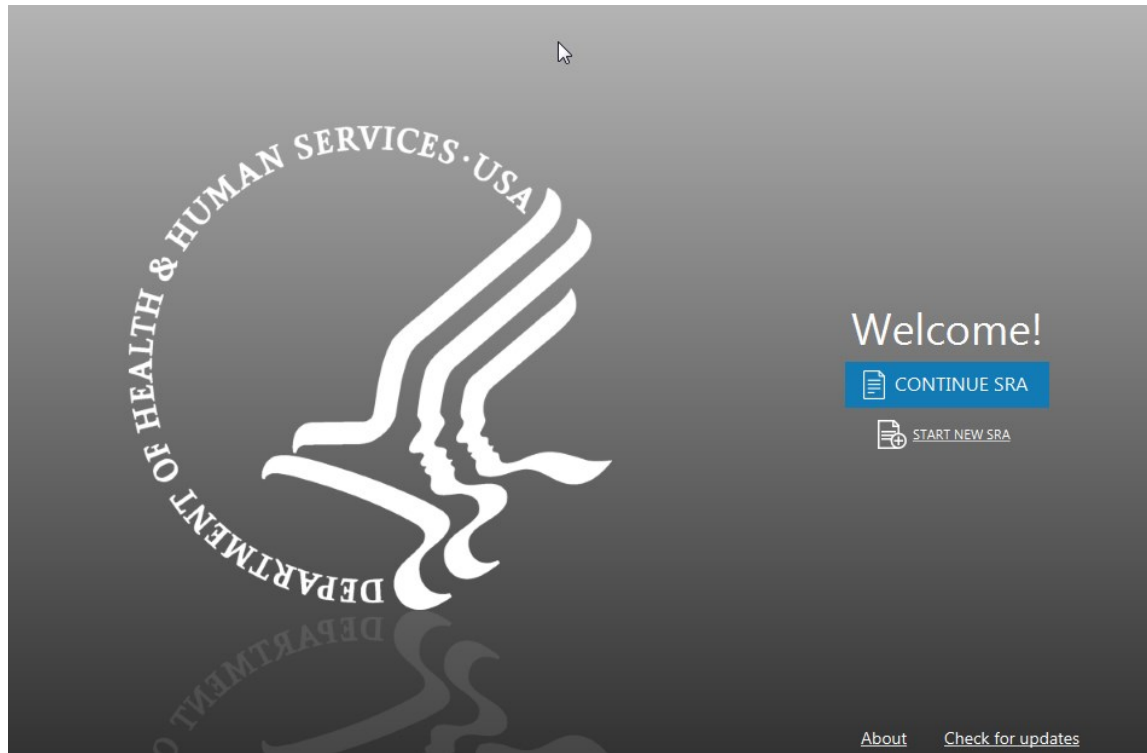
The tool runs on Windows, 7, 8, 10 and 11. All information entered into the tool is contained locally. No information is transmitted to DHHS, ONC or OCR.

Welcome Screen

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

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

The “Check for Updates” feature allows you to see if new content updates have been released by ONC.

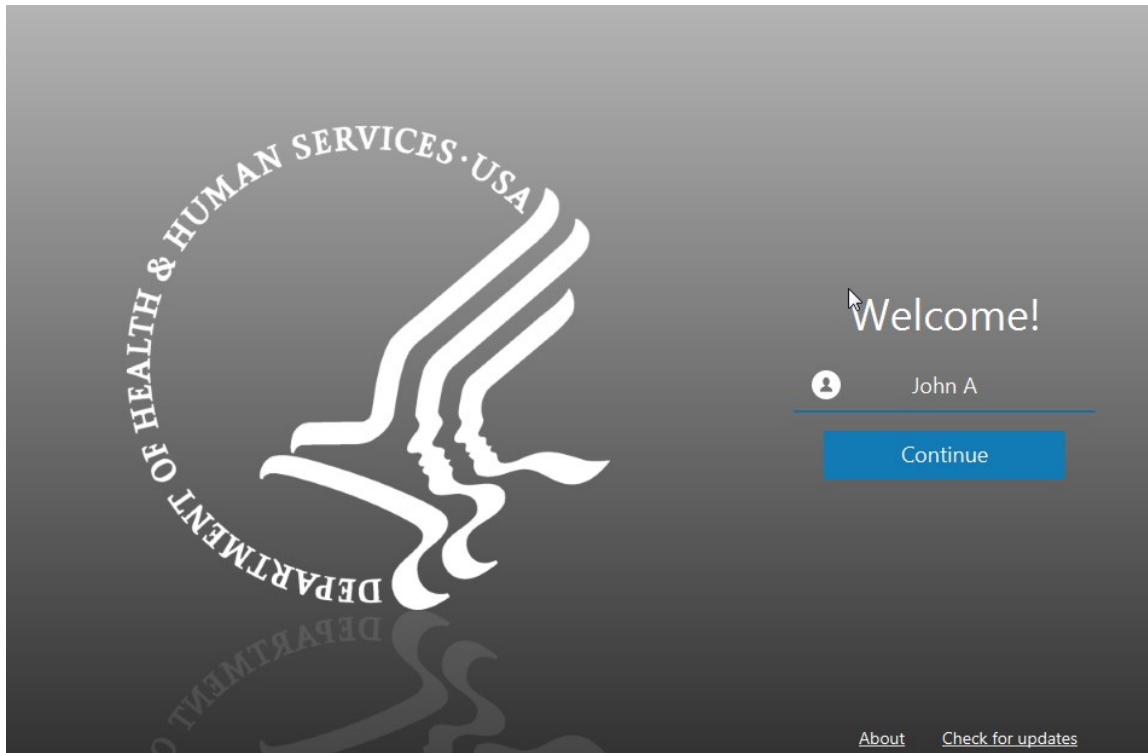


Entering a Username

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

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

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

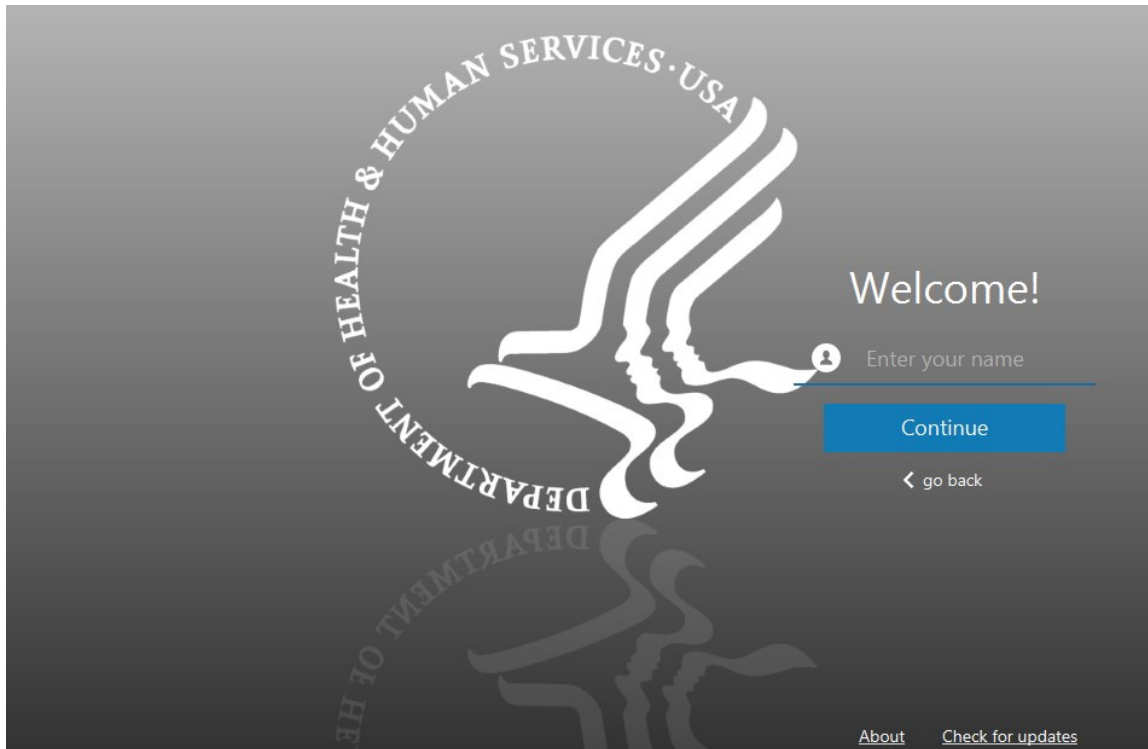


Saving a New SRA File

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

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

Files with the .sra extension can be opened and edited with the SRA Tool application.



The image shows two screenshots of the SRA (Security Risk Assessment) application interface. The top screenshot is the 'Practice Information' page, which includes a navigation sidebar on the left and a main content area with a form for adding practice information. The bottom screenshot is the 'Practice Assets' page, which includes a navigation sidebar on the left and a main content area with buttons for adding, downloading, exporting, and uploading asset templates, and a table for managing assets.

Practice Information

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:

Address:

City, State, Zip:

Phone, Fax:

Point of Contact:

Title/Role:

Phone:

Practice Assets

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 [0] | Manage Multiple

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

< Back | Next >

Practice Information, Asset & Vendor Management

A place to track:

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

Assessment

The screenshot displays the SRA Assessment interface. The top navigation bar includes the SRA logo, the title "Section 5: Security and the Practice", and icons for "practice", "assessment", and "summary". A left sidebar contains navigation options: Home, Practice Info, Assessment, Section 1-7, Reports, Save, Save As, and Logout. The main content area shows a question: "Q3. Do you restrict physical access to and use of your equipment [i.e. equipment that house ePHI]?". Below the question are four radio button options. To the right of the question are two panels: "Education" and "Reference". The "Education" panel contains text explaining that the selected option is the most effective for protecting ePHI. The "Reference" panel lists citations: HIPAA: §164.310(a)(1), NIST CSF: ID.RA, PR.AC, DE.CM, PR.IP, and HICP: TV1, Practice # 6. At the bottom of the question area is a "Details" field with a placeholder text and a "Back Next" button.

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.

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

Threats & Vulnerabilities

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

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

Each vulnerability comes with a list of related threats that must be rated for the **likelihood** they may occur and the **impact** they would have should they occur.

Security Risk Assessment

SRA Section 4: Complete!

practice assessment summary

Home Practice Info Assessment

Section 1 ✓ Section 2 ✓ Section 3 ✓ Section 4 ✓ Section 5 ✓ Section 6 ✓ Section 7 ✓ Summary Save Save As Logout

Congratulations you've completed Section 4, on Security & Data. Below is a summary highlighting where your practice is meeting the standard and potential areas of improvement.

Export

< Jump to section start

93% 7%

Areas of Success

- ▶ Q1. Do you manage and control personnel access to ePHI, systems, and facilities?
- ▶ Q2. How do you manage and control personnel access to ePHI, systems, and facilities?
- ▶ Q3. What is your process for authorizing, establishing, and modifying access to ePHI?
- ▶ Q5. How are individual users identified when accessing ePHI ?
- ▶ Q6. Do you ensure all of your workforce members have appropriate access to ePHI?
- ▶ Q7. How do you make sure that your workforce's designated access to ePHI is logical, consistent, and appropriate ?

Areas for Review

- ▶ Q4. How much access to ePHI is granted to users or other entities?
- ▶ Q27. Have you implemented mechanisms to record activity on information systems which create or use ePHI ?

Additional Information

Documents

Section Summary

Each section is concluded with a **Section Summary**. The **Section Summary** shows each of the questions answered, responses, and education content.

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

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

Reports

Risk Assessment

SRA Risk Report

practice assessment summary

Home Practice Info Assessment Reports Risk Report Detailed Report Flagged Report Remediation Rep... Glossary Save Save As Logout

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

Risk Breakdown

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

▼ Vulnerabilities

Section 1: SRA Basics

Vulnerabilities & Threats

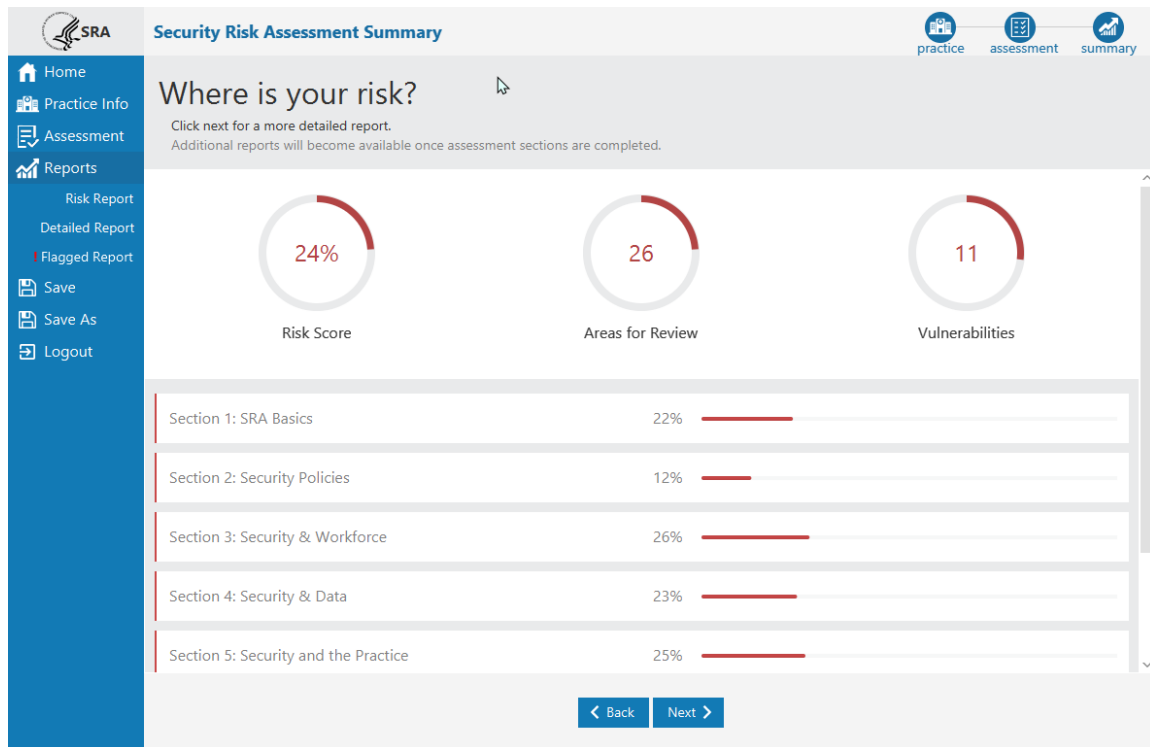
Inadequate risk awareness or failure to identify new weaknesses

Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches Low

Physical threats such as unauthorized facility access,

< Back Next >

Version Information



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.

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.

Risk Breakdown

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

Vulnerabilities

Section 1: SRA Basics
Vulnerabilities & Threats

Inadequate risk awareness or failure to identify new weaknesses

Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches Low

Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardous materials (chemicals, magnets, etc.) Low

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

Risk Report

The Risk Report displays the selected Vulnerabilities and Threat Ratings, as well as, all questions that were sorted into “Areas for Review”.

Users can review the question, their answer, and the education guidance so they know how to improve their security and mitigate risk in that area.

The screenshot shows the 'Risk Report' interface. At the top, there are navigation icons for 'practice', 'assessment', and 'summary'. Below the header, a message reads: 'Understand your security risk assessment by reviewing the matrix below. Click within each section to view your areas of review and corrective action plans.' An 'Export' button is also present. A dropdown menu labeled 'Areas for Review' is expanded, showing a table with the following data:

Section	Question	Your Answer	Education	References
1	Q3. How often do you review and update your SRA?	Periodically but not in response to operational changes and/or security incidents.	An accurate and thorough security risk assessment should be reviewed and updated periodically, or in response to operational changes, or security incidents.	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR, IP, RS.MI HICP: N/A
1	Q6. What do you include in your SRA documentation?	Our SRA documentation includes possible threats and vulnerabilities which we assign impact and likelihood ratings to. This allows us to determine severity. We do not include corrective action plans.	Corrective action plans should be developed as needed to mitigate identified security deficiencies according to which threats and vulnerabilities are most severe. Establish a data classification policy that categorizes data as, for example, Sensitive, Internal Use, or Public Use. Identify the types of records relevant to each category. Organizational policies should address all user interactions with sensitive data and reinforce the consequences of lost or	HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR, IP, RS.MI HICP: TV1, Practice # 4, 5, 9

At the bottom of the table, there are 'Back' and 'Next' navigation buttons.

Detailed Report

The Detailed Report is a collection of all data captured throughout the entire assessment.

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

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

SRA 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**

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 >

What to Expect

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

Enhancements in Version 3.4

The screenshot displays the 'Remediation Report' interface within a 'Risk Assessment' application. The interface features a blue sidebar on the left with navigation options: Home, Practice Info, Assessment, Reports (with sub-items: Risk Report, Detailed Report, Flagged Report, Remediation Rep...), Glossary, Save, Save As, and Logout. The main content area is titled 'Remediation Report' and includes a description: 'The Remediation Report provides a space to record responses to deficiencies in process or policies identified in your risk assessment. Items for review can be assigned an owner, due date, and date completed. [Learn more about documenting remediations...](#)' and an 'Export' button. Below this is a section navigation bar showing 'Sections: < 1 2 3 4 5 6 7 >' and 'now showing Section 1, (3) records' with '0/3 Remediations Completed - Section 1'. The current section is 'Section 1: SRA Basics'. Two questions are visible: 'Q3: How often do you review and update your SRA?' and 'Q4: Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?'. Each question has an 'Answer' field, an 'Education' section, and a 'References' section. For Q3, the answer is 'Only in response to operational changes and/or security incidents', education states 'An accurate and thorough security risk assessment should be reviewed and updated periodically, or in response to operational changes, or security incidents.', and references include 'HIPAA: §164.308(a)(1)(ii)(A)', 'NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR.IP, RS.MI', and 'HICP: N/A'. For Q4, the answer is 'No.', education states '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', and references include 'HIPAA: N/A', 'NIST CSF: ID.RA, PR.DS, ID.AM', and 'HICP: TV1, Practice # 5'. Buttons for 'Add Remediation' and '< Back' are present at the bottom of the content area. The bottom of the sidebar contains a 'Version Information' link.

SRA Glossary

practice assessment summary

- Acceptable Risk** - The level of risk that is considered acceptable. It implies that the potential harm or negative impact associated with the risk is deemed reasonable or manageable.
- Access Control** - Restrictions placed on access to systems or data someone is allowed to have. Access controls determine what information, areas, or functions a person can access based on their role, responsibilities and clearance. Access control levels are set to maintain security, privacy, and control over sensitive information.
- Access List** - A list that defines permissions to access systems, data, or other resources. The access list ensures that only authorized individuals are granted access while preventing unauthorized access.
- Administrative Safeguards** - The rules and actions put in place by an organization to keep information safe and ensure business operations run smoothly. These safeguards include activities such as creating and enforcing policies, training employees, and establishing processes to protect sensitive data and maintain security.
- Asset** - Something valuable to an organization. It can be physical, intangible, financial, or digital. Examples of assets relevant to small to medium sized practices include: computers, mobile devices, network devices, and software. Assets can include more than just physical devices.
- Audit** - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.
- Back-Up** - A copy of files and programs made to facilitate recovery if necessary.
- Business Associate** - A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity or another business associate.
- Compromise** - The unauthorized disclosure, modification, substitution, or use of sensitive data (e.g., keys, metadata, or other security-related information) or the unauthorized modification of a security-related system, device or process in order to gain unauthorized access.
- Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Contingency Plan** - A plan to continue operations in case something unexpected happens. A contingency plan helps minimize negative impacts following an adverse event. It involves identifying potential problems or risks and creating a plan of steps or actions to take to continue operations should these problems occur.
- Continuous Monitoring** - Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Version Information

Glossary

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

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

Security Risk Assessment

SRA Section 1: SRA Basics

practice assessment summary

Home Practice Info Assessment

Section 1 Section 2 ✓ Section 3 ✓ Section 4 ✓ Section 5 ✓ Section 6 ✓ Section 7 ✓

Reports Glossary Save Save As Logout

Version Information

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

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

Education

Continuing to complete security risk assessments will help safeguard confidential availability scheduling to improve

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Reference

HIPAA: §164.308(a)(1)(ii)(A)
NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI
HICP: TV1, Practice # 7, 10

► Details:

< Back Next >

Remediation Report

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

SRA Remediation Report

The Remediation Report provides a space to record responses to deficiencies in process or policies identified in your risk assessment. Items for review can be assigned an owner, due date, and date completed. [Learn more about documenting remediations...](#)

Sections: < 1 2 3 4 5 6 7 > now showing Section 2, (2) records 0/2 Remediations Completed - Section 2

Section 2: Security Policies

Q4: Is the security officer involved in all security policy and procedure updates?

Answer: No.

Education
You should have a designated security officer and any/all policy or procedure updates should be reported to the security officer. Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for implementing security practices and setting and establishing policy.

References
HIPAA: §164.316(b)(2)(ii)
NIST CSF: ID.GV, ID.RA, PR.IP, RC.IM, RS.IM
HICP: TV1, Practice # 10

Remediation Activities:

Owner: Due Date: Date Completed: + Link Document **Save Remediation**

< Back

HICP 2023 Edition Updates

The screenshot displays the SRA assessment interface. The top navigation bar includes 'Section 1: SRA Basics' and icons for 'practice', 'assessment', and 'summary'. A left sidebar contains navigation options: Home, Practice Info, Assessment, Section 1-7 (all with checkmarks), Reports, Save, Save As, and Logout. The main content area shows question Q4: 'Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?'. A popup window titled 'Learn more...' is open, showing an information icon, 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.', a link to 'HHS.gov - HICP Technical Volume 1', and an 'Ok, got it!' button. The popup also features a 'Reference' section with the following text: 'HIPAA: N/A', 'NIST CSF: ID.RA, PR. DS, ID.AM', and 'HICP: TV1, Practice # 5'. At the bottom of the main content area, there are 'Back' and 'Next' buttons.

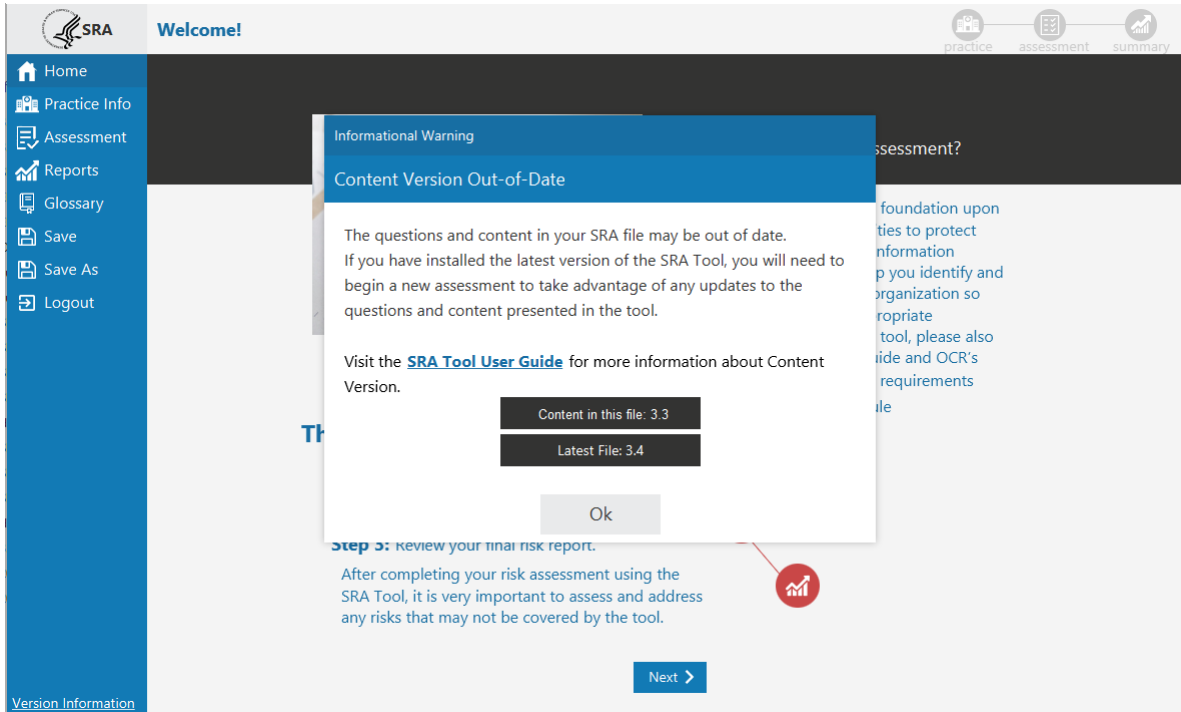
References updated for HICP 2023 Edition.

- New references added
- Links updated

Content Version Warning

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

Must be dismissed each time old file is opened.



The image displays two screenshots of the SRA (Security Risk Assessment) tool interface. Both screenshots show a question: "Q1. Has your practice completed a security risk assessment (SRA) before?".

Top Screenshot: The interface includes a navigation sidebar on the left with options like Home, Practice Info, Assessment, and Reports. The main content area has a question with radio button options: Yes (selected), No, I don't know, and Flag this question for later. To the right, there is an "Education" pane with text: "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." Below this pane is a "Copy text to clipboard" button.

Bottom Screenshot: This screenshot shows the same question and options. The "Education" pane is now enclosed in a dashed border, and a "Reference" pane is visible below it, containing text: "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". A green notification bubble says "Text copied." at the bottom center of the question area.

Copy Text, and others...

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

Excel Workbook

Released initially with SRA Tool Version 3.3.

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

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		
			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:									
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	High		

Conducting a Thorough Assessment



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

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

Frequently Asked Questions

How do I upgrade to the latest version of the SRA Tool without starting over from scratch?

The installer is designed to overwrite the previous version of the tool without issue. Files created with previous versions of the tool will still work. However, if you continue working on older files, you may be missing out on content updates.

How do I update the Audit Date displayed in the Detailed Report.

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

Is SRA Tool available for Apple or Mac computers?

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

Does the SRA File or report need to be submitted anywhere?

Your SRA is for your own records. It may be required for an incentive program like MIPS, but that is outside of the scope of the tool. SRA files are not submitted to ONC or OCR.

Questions From Chat

The screenshot shows a web application window titled "Risk Assessment". The main content area is "Section 1: SRA Basics". A question, Q10, asks: "How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?". There are five radio button options: "Written and verbal communication as well as coordinated corrective action planning.", "Written communication only.", "Verbal communication only.", "We do not communicate risk assessment results to workforce members.", and "Flag this question for later.". The "Written communication only." option is selected. To the right of the question are two red-bordered boxes: "Education" and "Reference". The "Education" box contains text about communicating SRA results to personnel. The "Reference" box lists HIPAA, NIST CSF, and HICP. At the bottom of the question area is a "Details:" link. At the bottom of the application window are "Back" and "Next" buttons. A blue sidebar on the left contains navigation links: Home, Practice Info, Assessment, Section 1-7, Reports, Glossary, Save, Save As, Logout, and Version Information. The top right of the application window has "practice", "assessment", and "summary" tabs.

Risk Assessment

Section 1: SRA Basics

practice assessment summary

Q10. How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?

Written and verbal communication as well as coordinated corrective action planning.

Written communication only.

Verbal communication only.

We do not communicate risk assessment results to workforce members.

Flag this question for later.

Education

Written results of your SRA should be communicated to the personnel responsible for responding to identified threats and vulnerabilities but also consider involving the personnel responsible for responding to identified threats and vulnerabilities in the creation of corrective action plans.

Reference

HIPAA: §164.308(a)(1)(ii)(B)

NIST CSF: ID.RA, ID.RM, RS.MI

HICP: N/A

► Details:

< Back Next >

Version Information

Contact Us

Contact the SRA Tool Helpdesk:

Email: SRAHelpDesk@Altarum.org

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

Additional Information & Resources

- Visit [HealthIT.gov](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](https://twitter.com/ONC_HealthIT) on Twitter for updates on the SRA Tool