



The Office of the National Coordinator for
Health Information Technology

Safeguarding Health Information: Building Assurance through HIPAA Security - 2018

OCR & ONC Security Risk Assessment (SRA) Tool Walk-Through: New Features and
New Functionality

November 30, 2018



Privacy and Security: A Shared Responsibility



Health Care Providers

- Understand Rules
- Protect and Secure Information
- Educate Staff and Patients



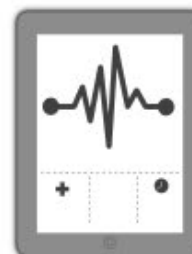
Government

- Promotes Trust
- Develops Policies
- Fairly Enforces Rules



Patients

- Understand Rights
- Protect Personal Information
- Be Engaged



Technology Vendors

- Embrace Privacy by Design
- Provide Convenient Technology
- Implement Standards

Security Risk Assessment (SRA) Tool

- The HHS Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR) have updated the popular [Security Risk Assessment \(SRA\) Tool](#) to make it easier to use and apply more broadly to the risks to health information.
- The tool is designed for use by small to medium sized health care practices – covered entities, and business associates to help them identify risks and vulnerabilities to ePHI.
- The updated tool provides enhanced functionality to document how such organizations can implement or plan to implement appropriate security measures to protect ePHI.
- Windows operating system- Download the Windows version of the tool at <http://www.HealthIT.gov/security-risk-assessment>.
- The iOS iPad version was not updated, but the previous version is available at the [Apple App Store](#) (search under “HHS SRA Tool”).

New Features and Functionality

- Enhanced User Interface
- Modular Workflow with Question Branching Logic
- Custom Assessment Logic
- Progress Tracker
- Improved Threats & Vulnerabilities Rating
- Detailed Reports
- Business Associate and Asset Tracking
- Overall Improvement of the User Experience

Additional Features

- Asset List/Vendor List import/export
- Accommodates Multi-Location Practices
- Document Tracking/Linking within Assessment Sections or within Documents Section [aggregates documents]
- Audit Logging Across User Accounts
- Dynamic Content within Assessment
- Wizard-based Branching Logic within Assessment
- Risk Guided Framework

SRA Tool Development Approach

- ONC and OCR conducted comprehensive usability testing of the SRA tool (version 2.0) with health care practice managers.
- Analysis of the findings across the user base informed the development of the content and the requirements for the SRA Tool 3.0.
- ONC and OCR then conducted testing of the SRA tool 3.0 to compare the user experience in completing the same tasks presented in the first round of testing.
- Over the next year, ONC and OCR will continue to gather feedback on the tool to inform future SRA tool modifications and updates. You can give feedback or request help by visiting www.healthit.gov/form/healthit-feedback-form and selecting the “Security Risk Assessment (SRA) Tool” category.

SRA Tool Brief Overview- Content

- 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)

Important Reminder!

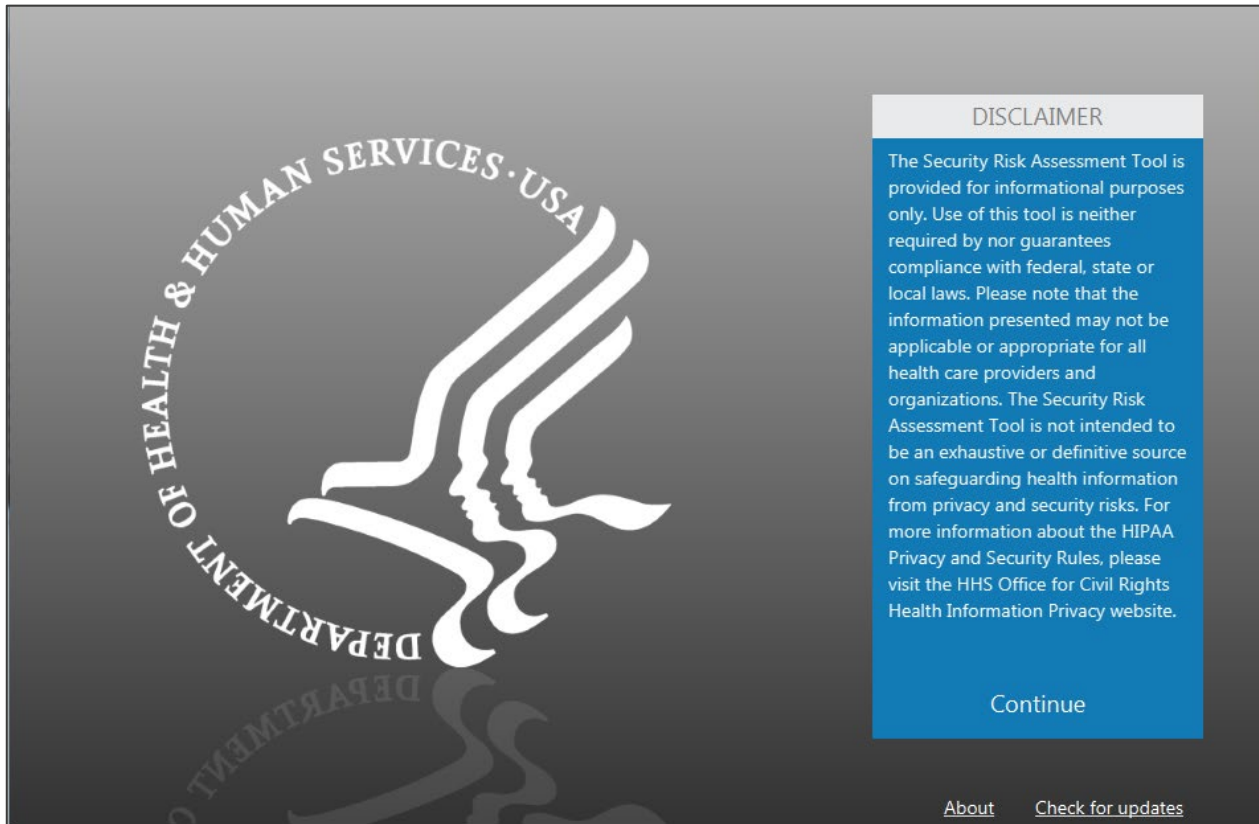
The SRA Tool runs on your computer. It does not transmit information to the Department of Health and Human Services, The Office of the National Coordinator for Health IT, or The Office for Civil Rights.

Top 10 Myths of Security Risk Analysis

1. The security risk analysis is optional for small providers.
2. Simply installing a certified EHR fulfills the security risk analysis MU requirement.
3. My EHR vendor took care of everything I need to do about privacy and security.
4. I have to outsource the security risk analysis.
5. A checklist will suffice for the risk analysis requirement.

Top 10 Myths of Security Risk Analysis

6. There is a specific risk analysis method that I must follow.
7. My security risk analysis only needs to look at my EHR.
8. I only need to do a risk analysis once.
9. Before I attest for an EHR incentive program, I must fully mitigate all risks.
10. Each year, I'll have to completely redo my security risk analysis.



- Enter your name
- Pick a place to save your SRA
- Name your SRA
- **Review the Disclaimer**
- Begin your SRA

SRA Welcome!

practice assessment summary

Home
Practice Info
Assessment
Summary
Save
Logout

What's a Security Risk Assessment?

A risk assessment is the first step in your Security Rule compliance efforts. Following HIPAA risk assessment guidelines will help you establish the safeguards you need based on the unique circumstances of your health care practice.

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 >

- Enter your name
- Pick a place to save your SRA
- Name your SRA
- Review the Disclaimer
- Begin your SRA

SRA Practice Information

practice assessment summary

Home Practice Info Assets Vendors Documents Assessment Summary Save Logout

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
Address
City, State, Zip
Phone, Fax
Point of Contact
Title/Role
Phone
Email

Delete Submit

+ another location

SRA Practice Information

practice assessment summary

Home Practice Info Assets Vendors Documents Assessment Summary Save Logout

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 Jackson Family Practice
Address 21 Main Street, Suite 201
City, State, Zip Grand Rapids MI 12345-9999
Phone, Fax 327-435-9999
Point of Contact Dr. David Jackson
Title/Role Primary Physician
Phone 327-435-9999
Email djackson@familypractice.com

saved ✓ Delete Submit

+ another location

< Back Next >

- **Practice Information**
 - » Track Asset Inventory
 - » Track BAA & Vendors
 - » Track Documentation

SRA Practice Assets

Home | Practice Info | Assets | Vendors | Documents | Assessment | Summary | Save | Logout

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

Add Asset (circled in red) | Download Asset Template | Export Asset List | Upload Asset Template

Total Assets [0]

Delete	Edit	ID #	Type	Status	ePHI	Encryption	Assignment
--------	------	------	------	--------	------	------------	------------

Add Asset

Asset Type: Desktop | Asset Status: Inactive [Storage] | ePHI Access: Maintains ePHI

Disposal Status: | Disposal Date: | Asset Encryption:

Asset Assignment: | Asset ID:

Comments:

SRA Practice Assets

Home | Practice Info | Assets | Vendors | Documents | Assessment | Summary | Save | Logout

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

Add Asset | Download Asset Template | Export Asset List | Upload Asset Template

Total Assets [1]

Delete	Edit	ID #	Type	Status	ePHI	Encryption	Assignment
Delete	Edit	DJ-0001	Laptop	Active [In-use a...	All of the above	Full disk encryp...	Dr. Jackson

< Back | Next >

- **Practice Information**
 - » Track Asset Inventory
 - » Track BAA & Vendors
 - » Track Documentation

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

Buttons: Add Vendor or BAA (circled in red), Download Vendor Template, Export Vendor List, Upload Vendor Template

Add Vendor [X]

Total Vendors [0]

Vendor Name:

Service Type Provided:

Vendor Address:

City, State, Zip:

Phone, Fax:

Contact Name/Title:

Contact Email:

+ Second Contact

Have satisfactory assurances been obtained?

Have additional risks been assessed?

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

Buttons: Add Vendor or BAA, Download Vendor Template, Export Vendor List, Upload Vendor Template

Total Vendors [1]

Delete	Edit	Vendor Name	Vendor Type	Satisfactory Assurance...	Risks Assessed
Delete	Edit	ABC Consultants	Consulting	Yes	Yes

Buttons: Back, Next

- **Practice Information**
 - » Track Asset Inventory
 - » Track BAA & Vendors
 - » Track Documentation

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
Summary
Save
Logout

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

Yes.
 No.
 I don't know.

Education
Performing a security risk assessment periodically will help safeguard the confidentiality, integrity, and availability of ePHI.

Standard
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 by the covered entity or

< Back Next >

- **Assessment Sections**

- » Wizard-based Logic
- » Multiple Choice Question & Answer format
- » Dynamic Education content
- » Related Standard Language

- **Progress Indicators**

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
Section 8
Summary
Save
Logout

Select the [vulnerabilities](#) that apply to your practice from the list below. Then rate the likelihood and impact on your practice of each potential [threat](#).

- Inadequate risk awareness
- Failure to remediate known risk
- Failure to identify new weaknesses
- Failure to meet minimum regulatory requirements and security standards
- Withholding Risk Assessment Results Information
- Asset Identity Awareness
- Unspecified workforce security responsibilities

< Back Next >

- Multi-Select format
- Guidance within ToolTips

SRA Section 5: Security and the Practice

practice assessment summary

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

Select the vulnerabilities that apply to your practice from the list below. Then rate the likelihood and impact on your practice of each potential threat.

✓ Inadequate procedures for managing facility access where information systems reside

	Likelihood			Impact		
Inability to review facility access logs	L	M	H	L	M	H
Inability to track and monitor staff/visitors/guests throughout facility	L	M	H	L	M	H
Increased response time to respond to facility security incidents	L	M	H	L	M	H
Unstructured guidance during facility access decision making	L	M	H	L	M	H

✓ Lacks protective measures to prevent physical viewing of ePHI and or sensitive information on computer systems

	Likelihood			Impact		
Access granted to unauthorized personnel	L	M	H	L	M	H
Disclosure of passwords and or login information	L	M	H	L	M	H

- Likelihood & Impact Rating

- » Color coded rating system

- » Guided Risk Framework

- Guidance within ToolTips

The screenshot displays the SRA dashboard interface. At the top, it indicates 'Section 1: Complete!' with a progress bar showing 75% completion (blue) and 25% remaining (red). Below this, a message congratulates the user for completing Section 1 and provides a summary of success and areas for improvement. The dashboard is divided into two columns: 'Areas of Success' and 'Areas for Review'. The 'Areas of Success' column lists five questions (Q2-Q6) with right-pointing triangle icons, indicating successful completion. The 'Areas for Review' column lists two questions (Q7 and Q10) with right-pointing triangle icons, indicating areas needing attention. A left-hand navigation menu includes options for Home, Practice Info, Assessment (with sub-sections 1-8), Summary, Save, and Logout. The top navigation bar includes icons for practice, assessment, and summary.

- Section Summary
 - » Areas of Success
 - » Areas for Review
 - » Score
 - » Comments & Documents

- Final SRA Summary
 - » Dashboard
 - » Detailed Report

SRA Section 1: Complete!

practice assessment summary

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.

75% 25%

Areas of Success

- ▶ Q2. Has your practice completed a security risk assessment (SRA) before?
- ▶ Q3. Do you review and update your SRA?
- ▶ Q4. How often do you review and update your SRA?
- ▶ Q5. Do you include all information systems containing, processing, and/or transmitting in your SRA?
- ▶ Q8. Do you respond to the threats and vulnerabilities identified in your SRA?
- ▶ Q9. Do you identify specific personnel to respond to and mitigate the threats and vulnerabilities found in your SRA?

Areas for Review

- ▶ Q7. What do you include in your SRA documentation?
- ▶ Q10. Do you communicate SRA results to personnel involved in responding to threats or vulnerabilities?

▼ Q7. 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 do not include corrective action plans.

Education: Corrective action plans should be developed as needed to mitigate identified security deficiencies according to which threats and vulnerabilities are most severe.

- Section Summary
 - » Areas of Success
 - » Areas for Review
 - » Score
 - » Comments & Documents
- Final SRA Summary
 - » Dashboard
 - » Detailed Report



- **Section Summary**

- » Areas of Success
- » Areas for Review
- » Score
- » Comments & Documents

- **Final SRA Summary**

- » Dashboard
- » Detailed Report



- **Summary Dashboard**
 - » Cumulative Risk score
 - » Risk score by section
 - » Total Areas for Review
 - » Total # of Vulnerabilities

SRA Detailed Report

Click each section to expand and review more details.

- ▶ Section 1, SRA Basics Risk Score: 22%
- ▶ Section 2, Security Policies Risk Score: 62%
- ▶ Section 3, Security & Workforce Risk Score: 16%
- ▶ Section 4, Security & Data Risk Score: 52%
- ▶ Section 5, Security and...
- ▶ Section 6, Security & w...
- ▶ Section 7, Contingency

Practice Information (2 loca...)

Practice Name
Address
City, State, Zip
Phone, Fax
Point of Contact
Title/Role
Phone
Email

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

SRA Detailed Report

Click each section to expand and review more details.

- ▶ Section 1, SRA Basics Risk Score: 22%
- ▼ Section 2, Security Policies Risk Score: 62%

Threats & Vulnerabilities Risk Rating

Uninformed Security Officer

- Adversarial access to ePHI Low
- Adversarial disruption of information system function High
- ePHI exfiltrated to unauthorized entities Medium
- Insider carelessness causing disruption Medium
- Insider carelessness exposing ePHI Medium

Question	Answer	Compliance Guidance/Rule	Username	Date/Time
Q0. Do you maintain documentation of policies and procedures regarding risk assessment, risk management and information security activities?	Yes, we have a process by which management develops, implements, reviews, and updates security policies and procedures.	Required	Lisa	Tue Jun 19 15:19:25 EDT 2018
Q1. Do you review and update your security documentation, including policies and procedures?	Yes, we review and update our security policies and procedures periodically or as needed, but not both.	Required	Lisa	Tue Jun 19 15:19:28 EDT 2018

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

- Detailed Report
 - » Risk scores for each section
 - » Audit Log
 - » Comprehensive report of SRA results
 - » Risk ratings for Threats & Vulnerabilities



The Office of the National Coordinator for
Health Information Technology



Questions?

www.healthit.gov/form/healthit-feedback-form



@ONC_HealthIT



@HHSOnc

HealthIT.gov 