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!

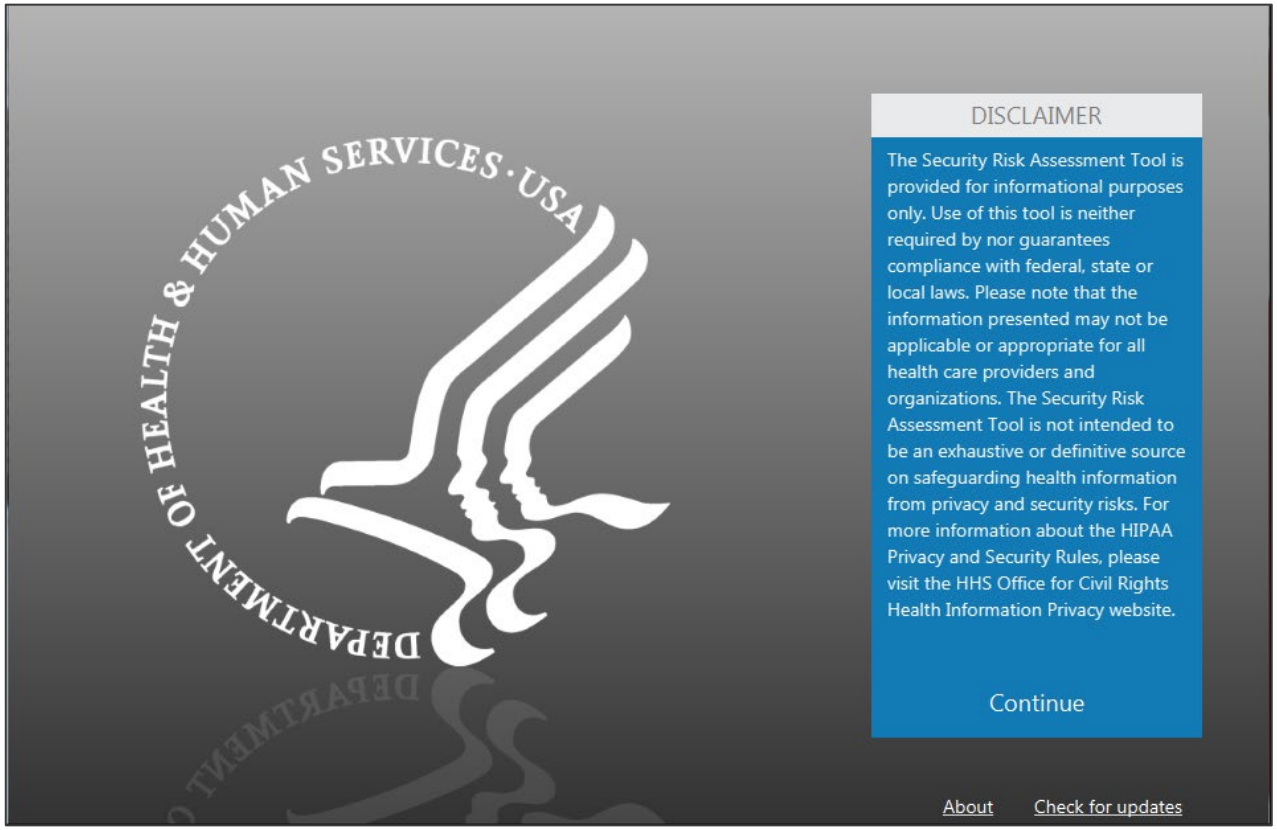
The SRA Tool runs on your computer. It does not transmit information to the Department of Health and Human Services, The Office of the National Coordinator for Health IT, or The Office for Civil Rights.

Top 10 Myths of Security Risk Analysis

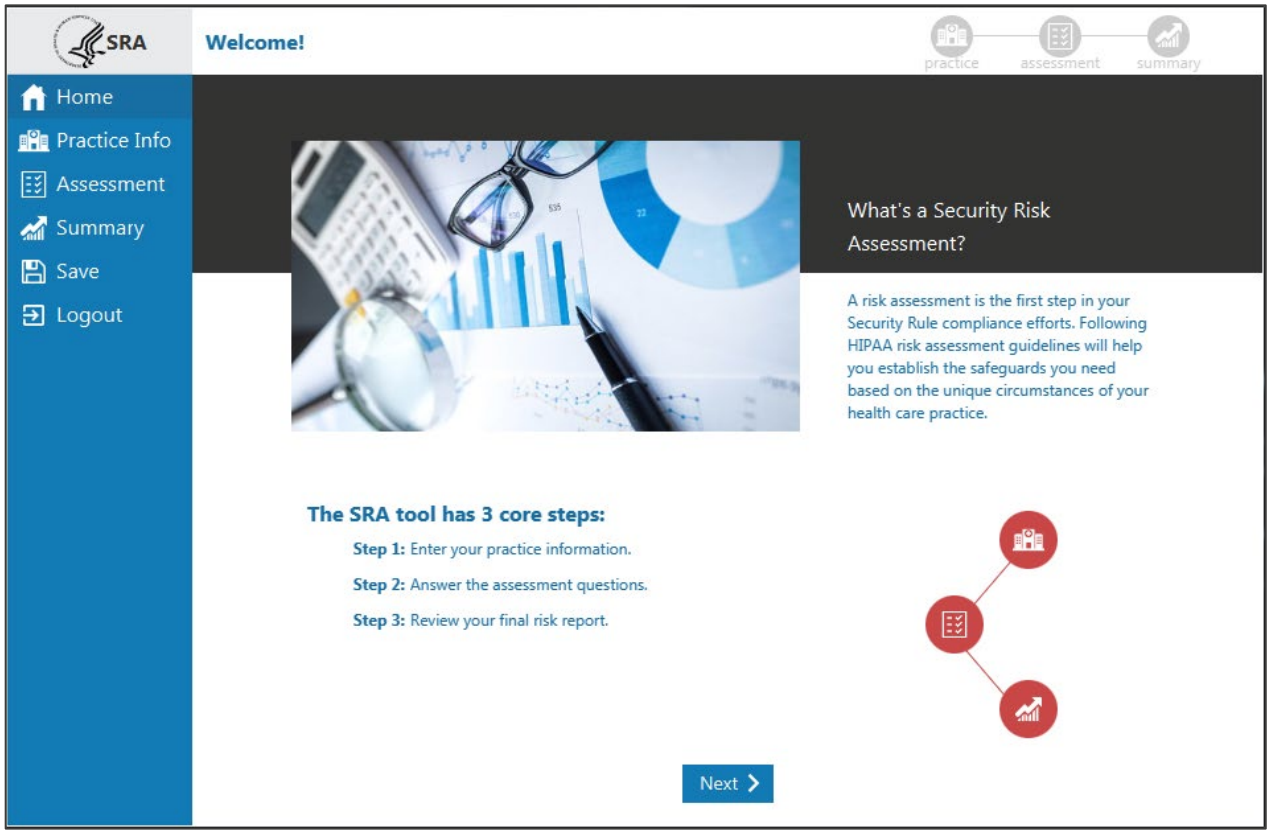
1. The security risk analysis is optional for small providers.
2. Simply installing a certified EHR fulfills the security risk analysis MU requirement.
3. My EHR vendor took care of everything I need to do about privacy and security.
4. I have to outsource the security risk analysis.
5. A checklist will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

Top 10 Myths of Security Risk Analysis

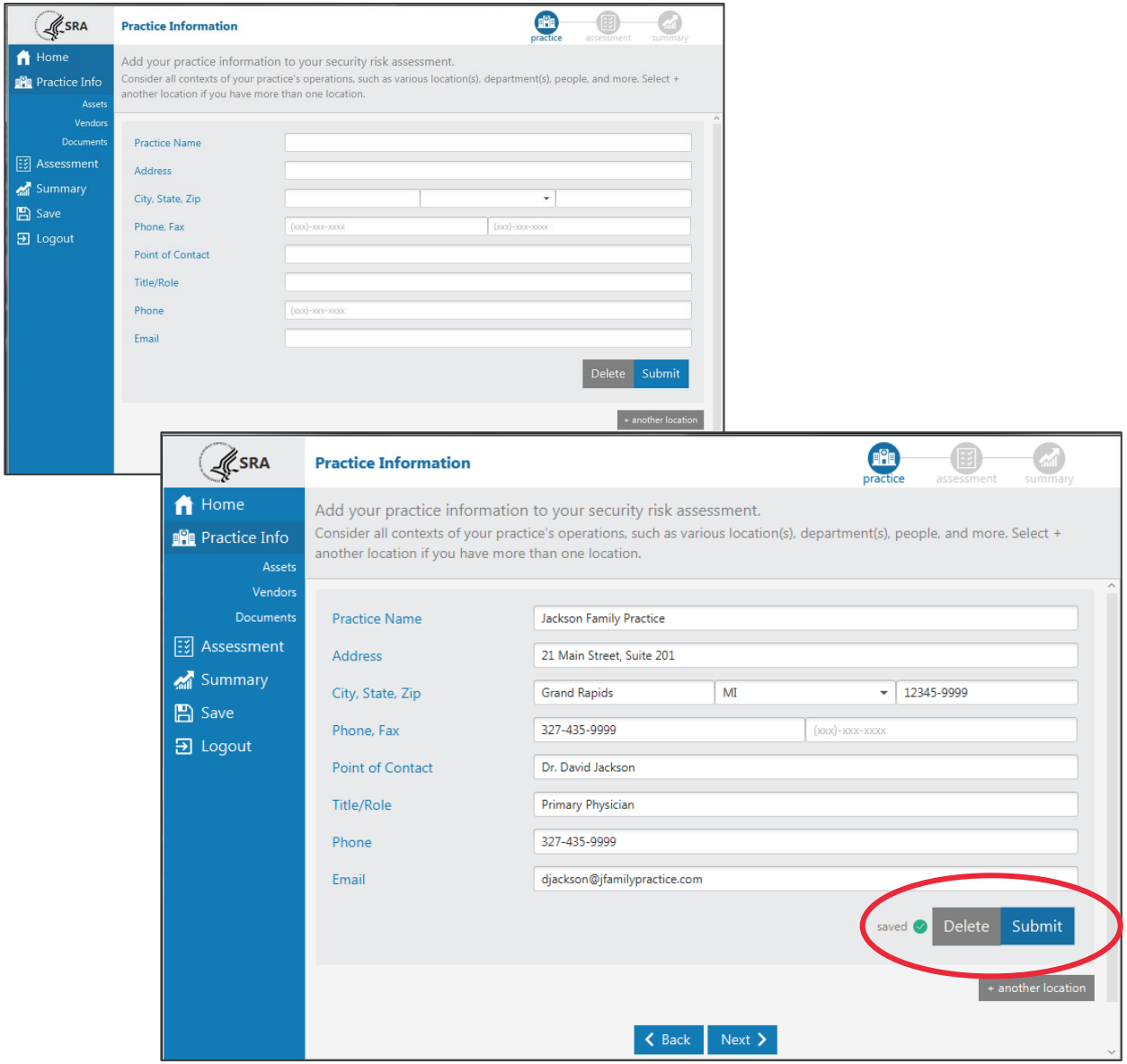
6. There is a specific risk analysis method that I must follow.
7. My security risk analysis only needs to look at my EHR.
8. I only need to do a risk analysis once.
9. Before I attest for an EHR incentive program, I must fully mitigate all risks.
10. Each year, I'll have to completely redo my security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



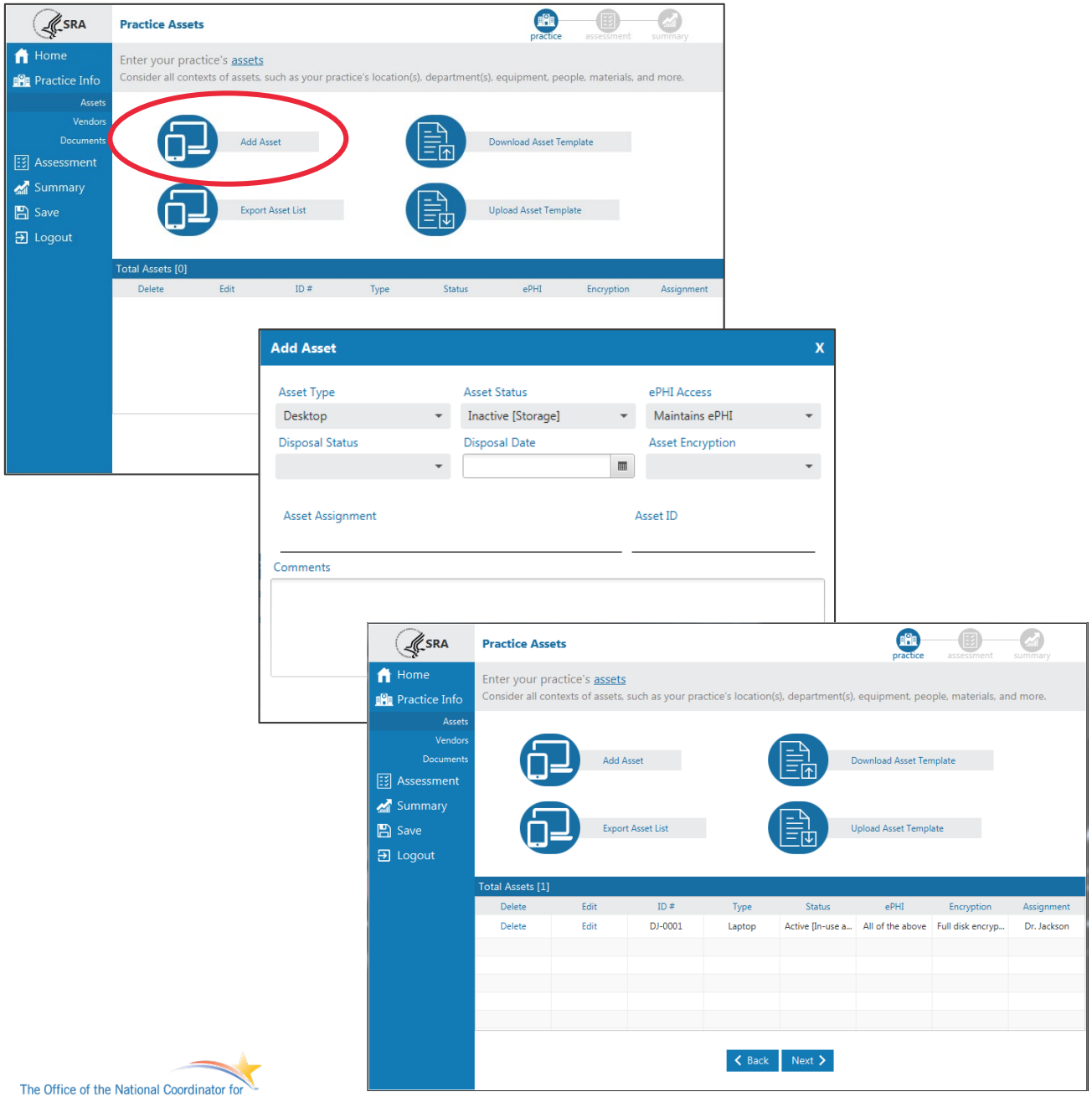
- Enter your name
- Pick a place to save your SRA
- Name your SRA
- **Review the Disclaimer**
- Begin your SRA



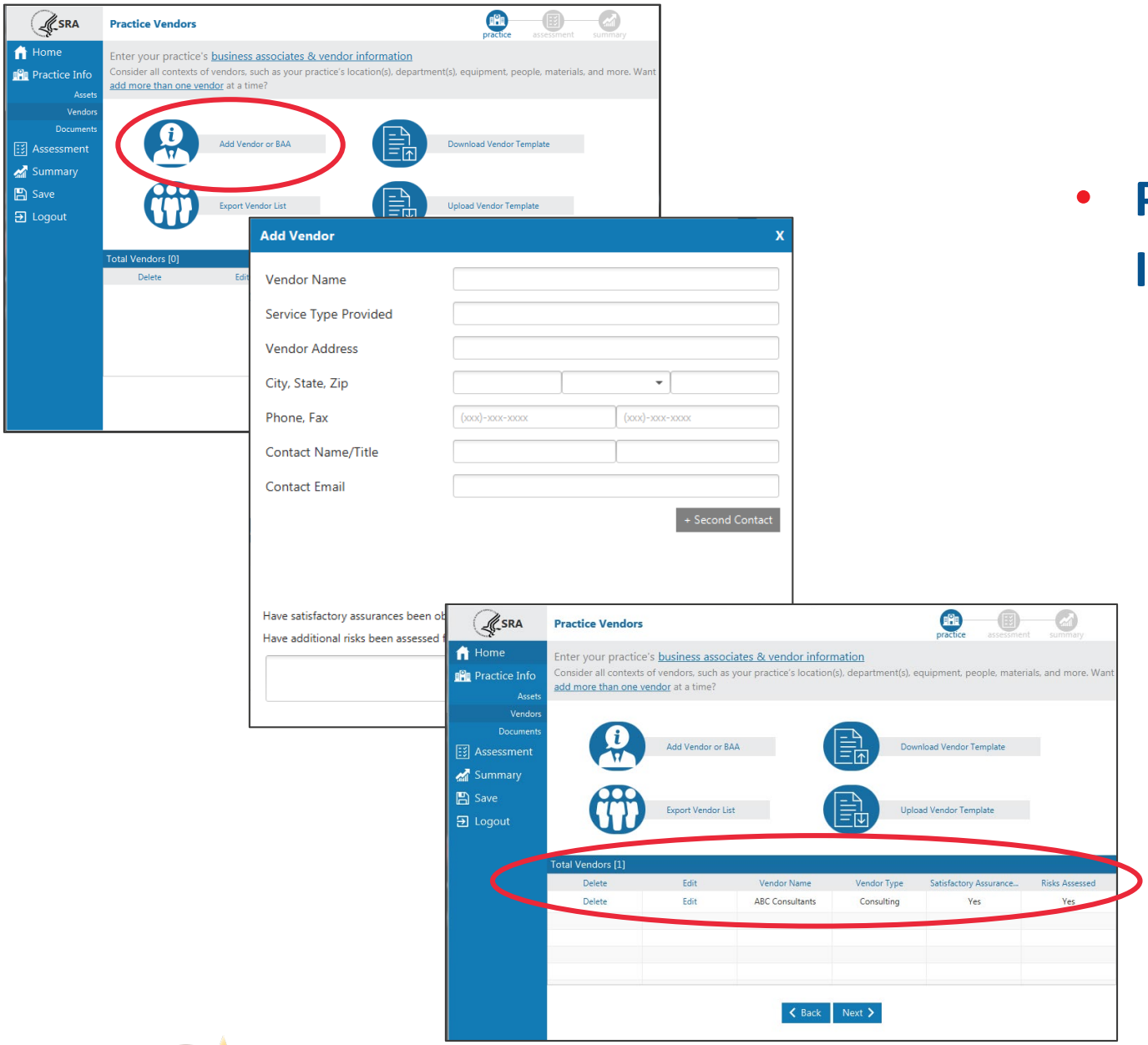
- Enter your name
- Pick a place to save your SRA
- Name your SRA
- Review the Disclaimer
- **Begin your SRA**



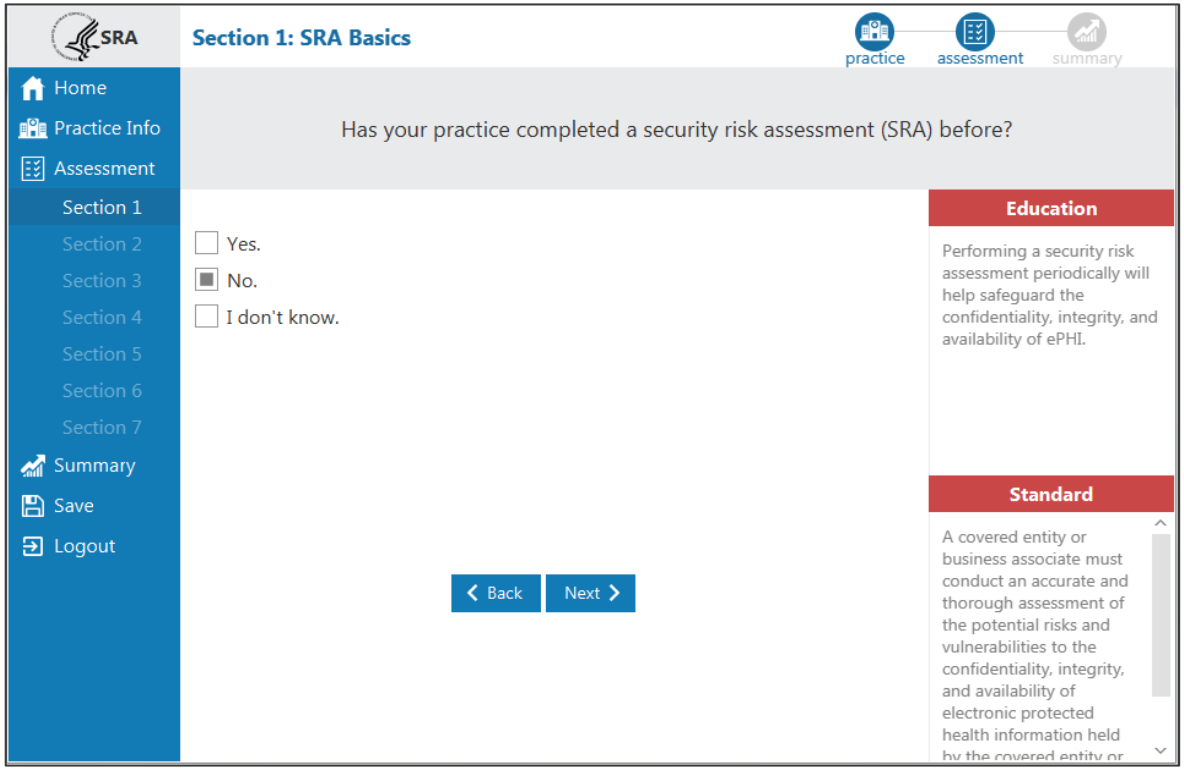
- **Practice Information**
  - » Track Asset Inventory
  - » Track BAA & Vendors
  - » Track Documentation



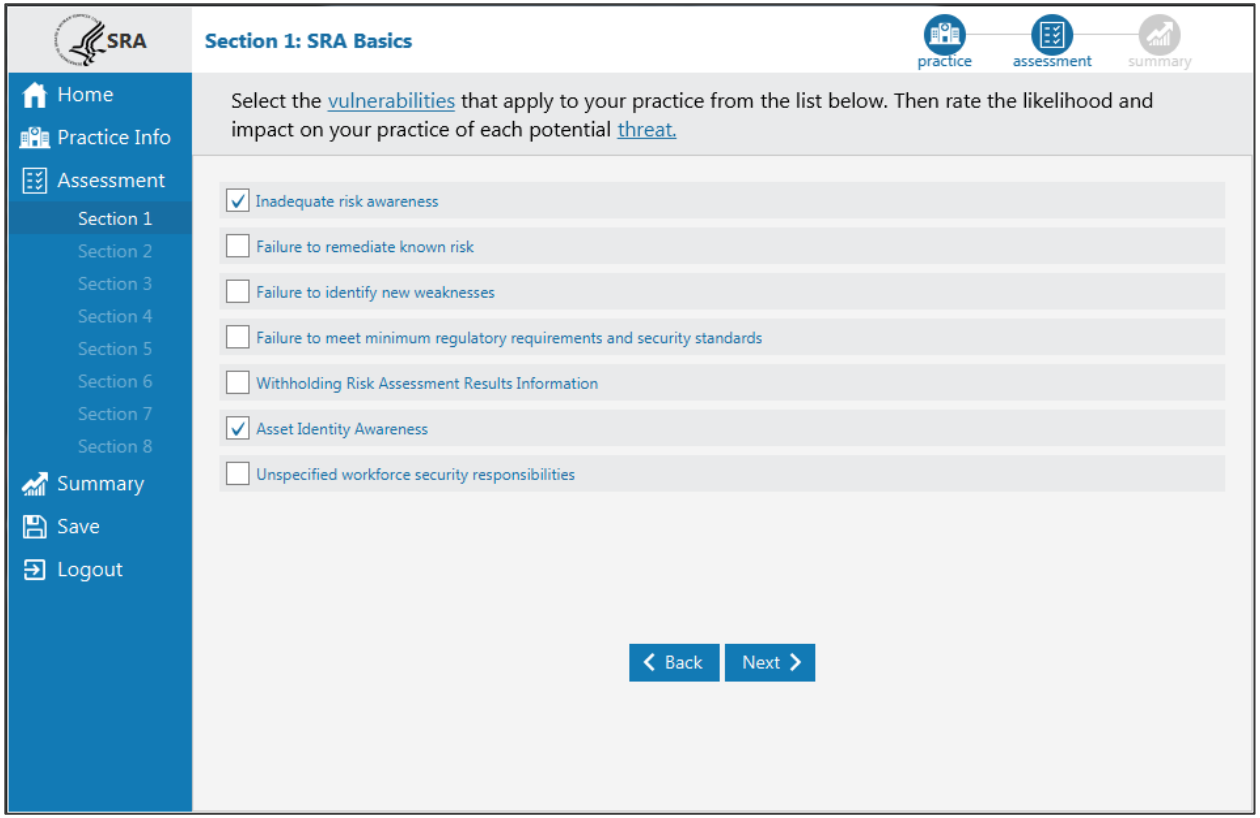
- **Practice Information**
  - » **Track Asset Inventory**
  - » Track BAA & Vendors
  - » Track Documentation



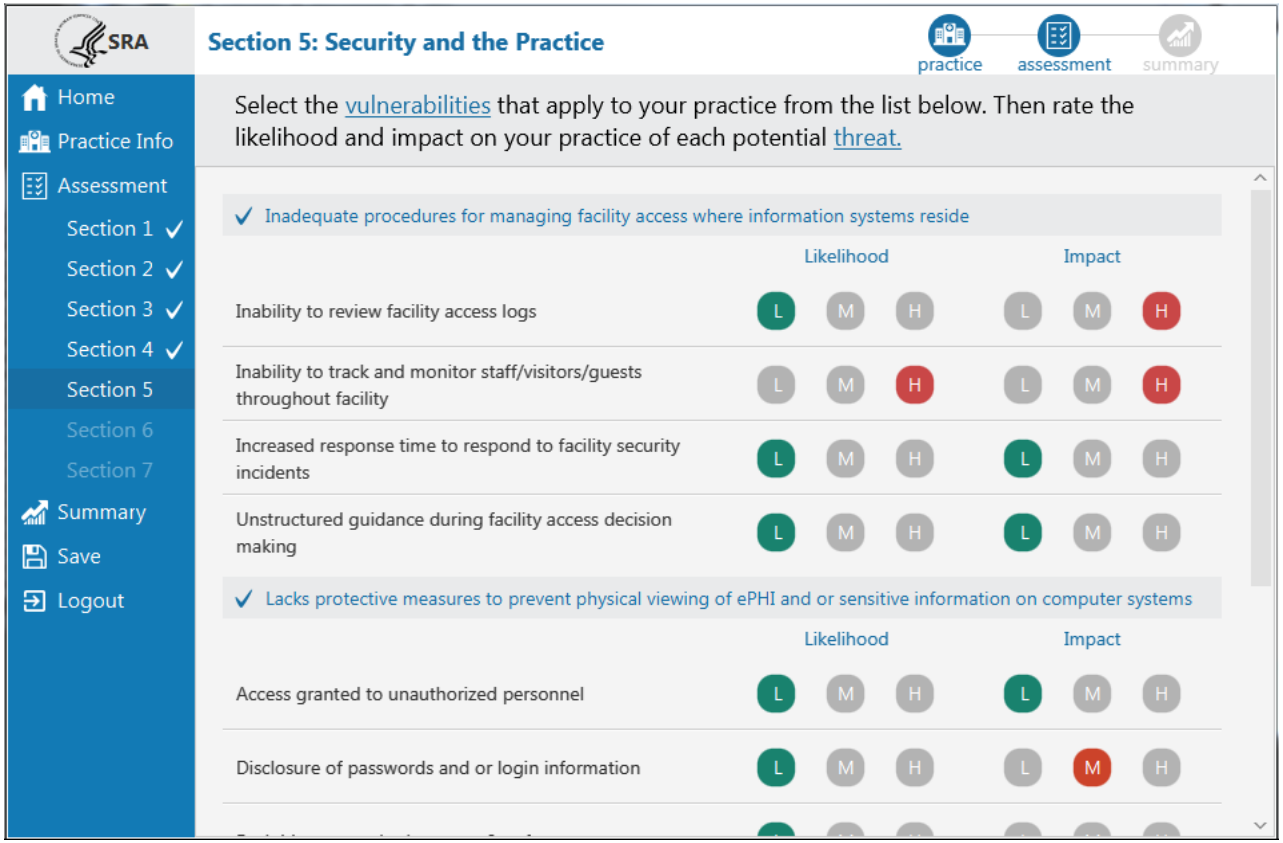
- **Practice Information**
  - » Track Asset Inventory
  - » **Track BAA & Vendors**
  - » Track Documentation



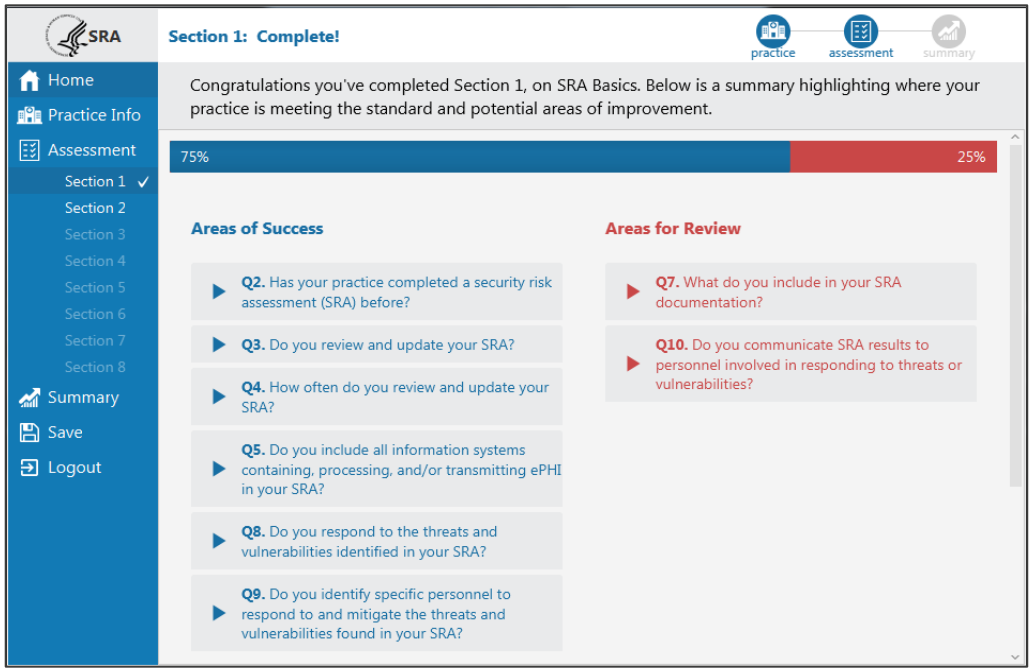
- **Assessment Sections**
  - » Wizard-based Logic
  - » Multiple Choice Question & Answer format
  - » Dynamic Education content
  - » Related Standard Language
- **Progress Indicators**



- Multi-Select format
- Guidance within ToolTips

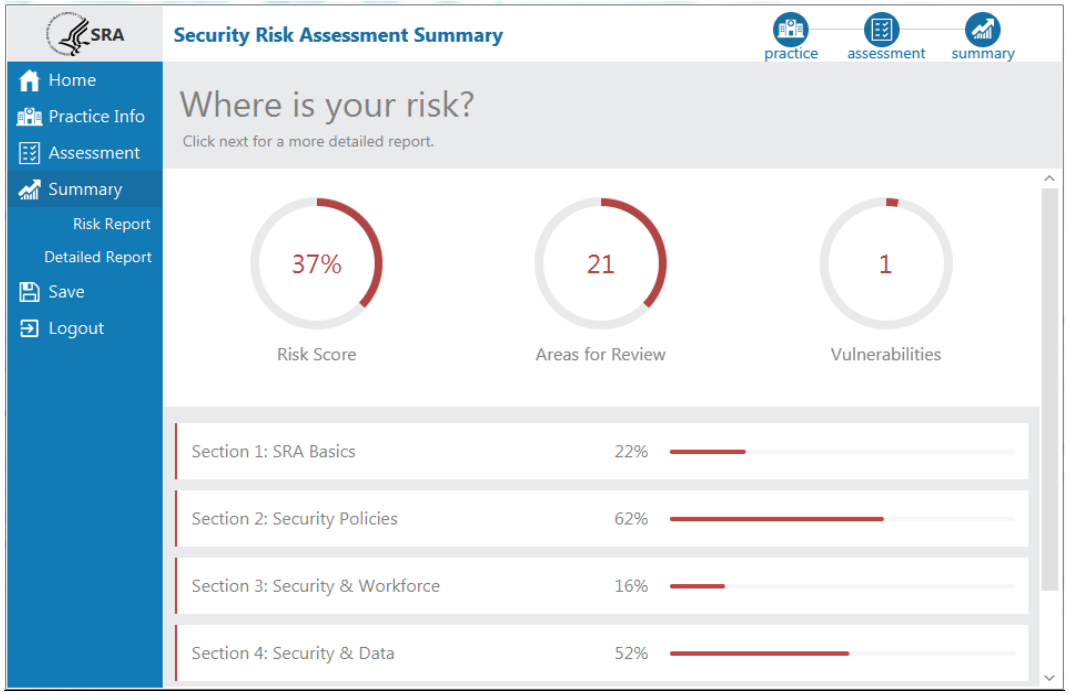


- Likelihood & Impact Rating
  - » Color coded rating system
  - » Guided Risk Framework
- Guidance within ToolTips

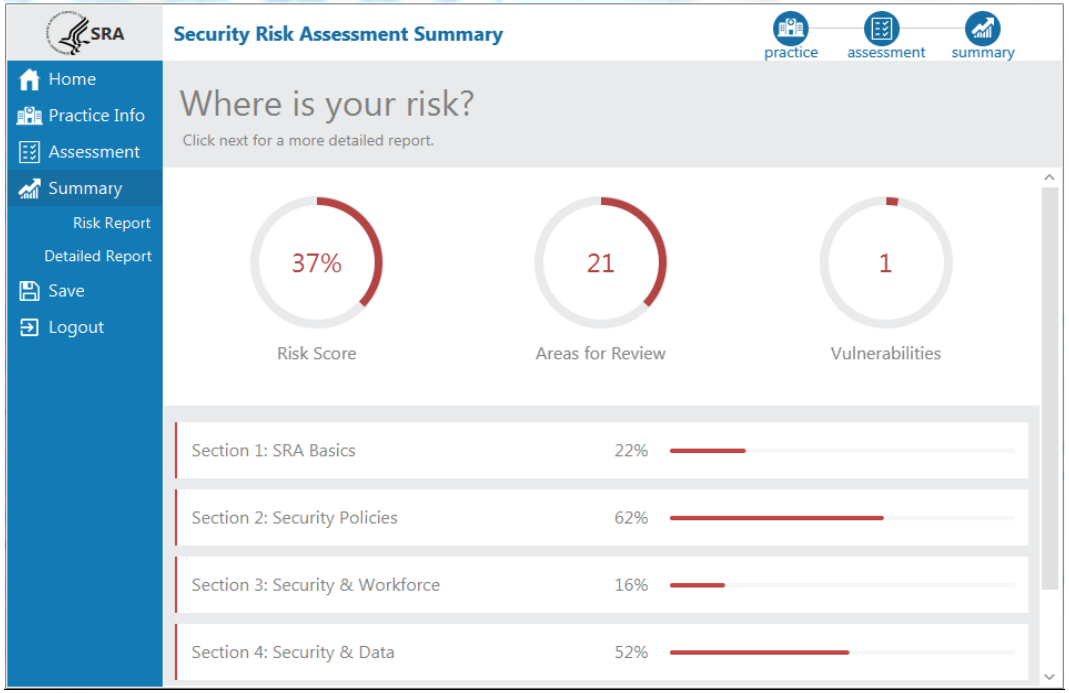


- Section Summary
  - » Areas of Success
  - » Areas for Review
  - » Score
  - » Comments & Documents
- Final SRA Summary
  - » Dashboard
  - » Detailed Report

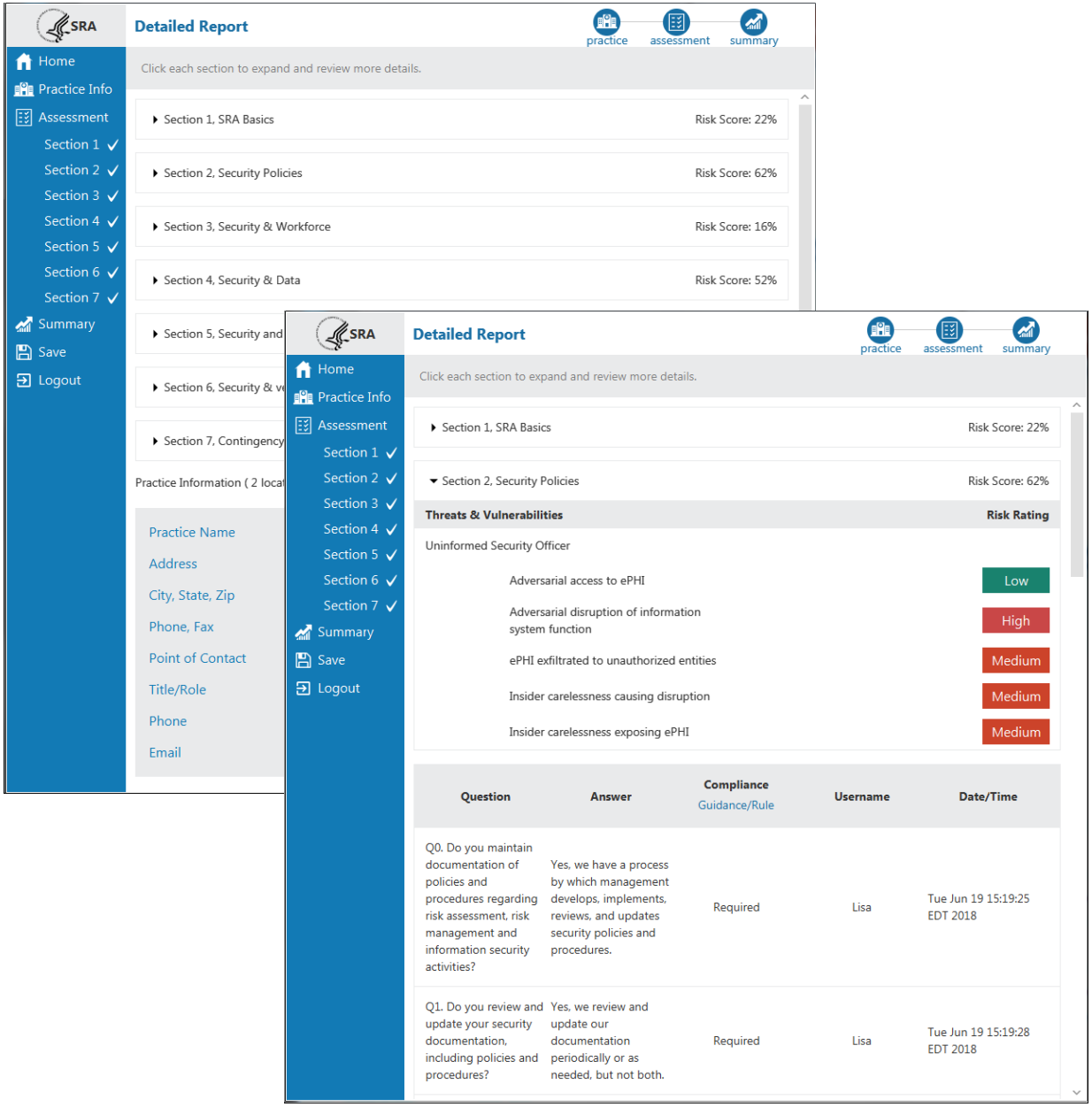
- Section Summary
  - » Areas of Success
  - » Areas for Review
  - » Score
  - » Comments & Documents
- Final SRA Summary
  - » Dashboard
  - » Detailed Report



- 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



- Detailed Report
  - » Risk scores for each section
  - » Audit Log
  - » Comprehensive r eport 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