U.S. Department of Health and Human Services (HHS)
The Office of the National Coordinator for Health Information Technology (ONC)

Security Risk Assessment (SRA) Tool User Guide

Version: 2.0
Date: September 2016

Contents

Acronym Index

Acronym	Definition
EHR	Electronic Health Record
ePHI	Electronic Protected Health Information
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act
NIST	National Institute of Standards and Technology
OCR	The Office for Civil Rights within HHS
ONC	The Office of the National Coordinator for Health Information Technology within HHS
OS	Operating System
PDF	Portable Document Format
PHI	Protected Health Information
SRA Tool	Security Risk Assessment Tool

1. Introduction

Welcome to the Security Risk Assessment Tool (SRA Tool), designed to help health care providers and business associates that handle patient information for them to evaluate risks, vulnerabilities and adherence to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The HIPAA Security Rule requires health care providers, health plans, and business associates to conduct risk analyses and implement technical, physical, and administrative safeguards for electronic protected health information (ePHI). The Office of the National Coordinator for Health Information Technology (ONC) worked together with the Office for Civil Rights (OCR), which enforces the HIPAA Security Rule, to develop this tool to enable providers and other entities to meet their HIPAA Security Rule compliance responsibilities.

We hope you find this tool helpful as you work towards improving the privacy and security of your health care practice and its compliance with the HIPAA Security Rule. Please remember that this is only a tool to assist in practice's review and documentation of a risk assessment. Therefore, this tool 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. The use of this tool does not mean that your practice is fully 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.

Note: This tool runs on your computer. None of the information you enter is reported to OCR or ONC through the tool.

1.1. Purpose

The purpose of the SRA Tool is to assist health care providers and their business associates in performing and documenting a Security Risk Assessment. The HIPAA Security Rule, effective since 2005, requires all organizations that are covered entities or business associates under HIPAA to conduct a thorough and accurate assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the entity (164.308(a)(1)(ii)(A)). As the health care industry is both diverse and broad, the HIPAA Security Rule is designed to be flexible and scalable.

1.2. Audience

This SRA Tool is designed for small to medium-sized practices and their business associates. ONC has historically defined small to medium-sized practices to be those with one to ten health care providers. This SRA Tool was designed to assist these smaller organizations in performing and documenting a risk assessment. While the tool may be helpful or informative for larger organizations, it may not account for the complexities sometimes found in such organizations, because the tool is intended for small organizations. Organizations should choose a security risk assessment tool and process that is right for them.

1.3. What is the SRA Tool?

The SRA Tool is a software application that a health care provider can use, along with other tools & processes, to assist in reviewing its implementation of the HIPAA Security Rule. The SRA Tool is available at no cost and can be used with several operating systems, including Microsoft Windows for desktop and laptop computers and Apple iOS for iPad. The iOS SRA Tool application for iPad can be downloaded from the Apple App Store. Section 2 provides instructions on how to download both versions of the SRA Tool.

The SRA Tool guides health care providers and business associates through the standards and implementation specifications identified in the HIPAA Security Rule and covers basic security practices, security failures, risk management, and personnel issues. Basic security practice questions include defining and managing access to systems and PHI, backups and data recoveries; and technical and physical security. Risk management questions address periodic reviews and evaluations and can include regular functions, such as continuous monitoring. Lastly, personnel issue questions address access to information as well as the on-boarding and release of staff as well as helping to identify areas where staff training may be appropriate, for example, not sharing passwords.

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

- HIPAA Security Rule[1]
- National Institute of Standards and Technology (NIST) Special Publication 800-66[2]
- NIST Special Publication 800-53[3]
- NIST Special Publication 800-53A[4]
- Health Information Technology for Economic and Clinical Health (HITECH) Act[5]

1.4. The Role of the SRA Tool in a Risk Assessment

The SRA Tool can support an organization's risk assessment process. Risk assessment identifies conditions under which ePHI could be disclosed without proper authorization, improperly modified, or made unavailable when needed. Responses to the questions in the SRA Tool can be used to help organizations identify areas where security controls and organizational policies designed to protect ePHI may need to be implemented or where existing implementations may need to be improved. Compliance with the Security Rule's risk analysis and risk management implementation specifications requires organizations to accurately and thoroughly assess the

---

[1] http://www.hhs.gov/hipaa/for-professionals/security/
[2] http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf
[5] https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf

potential risks and vulnerabilities to all of their ePHI, including ePHI on all forms of electronic media, and implement security measures that are sufficient to reduce these risks and vulnerabilities to a level that is reasonable and appropriate. If, after completing all of the questions in the SRA Tool, threats and vulnerabilities still exist but are unaccounted for in the SRA Tool (i.e., a particular threat or vulnerability did not fit well with any of the existing questions), the organization must either 1) document the unaccounted for threats and vulnerabilities and assess the risk posed in the most appropriate place within the SRA Tool, or 2) document the unaccounted for threats and vulnerabilities and assess the risk posed as part of a separate risk assessment document to supplement the SRA Tool. Using the tool will help you identify areas where you need to make changes to your security; the tool will not make those changes for you.

1.5. What the SRA Tool Is Not:

A Tool that Supports Multiple Concurrent Users. The SRA Tool is not intended to be, nor was it built to be, a collaborative tool to be used simultaneously by many users. It is expected that a single user at any one time with appropriate permissions to install and run the application on the computer will use the tool to individually capture information. However, multiple users may access the tool on separate occasions, and Version 2.0 of the tool allows the user to export a copy of the data entered into the tool and share with other users so that they may add additional information (see Sections 3.9 and 3.10). If you choose to use this feature you should ensure a single file is used since you cannot merge two different copies of the data.

A Guarantee of HIPAA Compliance. The SRA Tool does not produce a statement of compliance, nor does completion of the tool guarantee or otherwise indicate compliance with the HIPAA Security Rule or any other Federal, State, or local statutes. However, while the Tool will not prove you comply with the Security Rule in all respects, when completed in an accurate and thorough manner it can provide documentation of your organization's efforts to conduct a risk assessment, and this, in turn, is one of many aspects of security rule compliance that may be evaluated in an OCR audit or compliance review. Organizations may use the SRA Tool in coordination with other tools and processes to support risk analysis and risk management activities required by the HIPAA Security Rule. Statements of compliance are the responsibility of the covered entity and the HIPAA Security Rule regulatory and enforcement authority. Please note, the SRA Tool provides guidance in understanding the requirements of the HIPAA Security Rule—Risk Analysis specifically, and does not cover additional Security Rule requirements nor provisions for the HIPAA Privacy Rule.

2. Downloading the SRA Tool

2.1. Downloading the SRA Tool (Windows version)

To download the SRA Tool, for Microsoft Windows, navigate to ONC's website at: http://www.healthit.gov/security-risk-assessment (Figure 1).

Figure 1. HealthIT.gov/security-risk-assessment

Next, select the blue button located within the "Security Risk Assessment Tool" box (Figure 2).

Figure 2. SRA Tool Link Location

Once you select the button, you will be directed to the Security Risk Assessment Tool page. Navigate to the right side of the page to begin downloading the Windows version of the tool (Figure 3).

Figure 3. Windows-Version Download Link

While your downloading experience may vary depending upon the Internet browser you are using, all browsers should allow you to save the file on your desktop computer or laptop. Once prompted, select the arrow symbol next to the "Save" option and save the file to a location of your choice. Be sure to remember the location where you downloaded the file, as you will need to double click the file to run the tool.

2.2. Downloading the SRA Tool (iPad version)

To download the free SRA Tool onto your iPad, you will need to access the Apple App Store. The SRA Tool is currently not available for other Apple products such as the iPhone.

Within the App Store, you can find the SRA Tool by searching for "HHS SRA Tool." Select the "Free" button followed by the "Install" button to begin downloading the tool.

Downloading should begin automatically and should only take a couple of minutes depending on your Internet connection speed. Once the installation is complete, you will see the SRA Tool icon will appear on your iPad screen.

Select the SRA Tool icon to begin your assessment.

3. Using the SRA Tool

Once you have downloaded the application and saved it to your computer double-click the icon and select "run" when prompted. iPad users should tap the SRA Tool icon to launch the tool. The SRA Tool will open to the SRA Tool login screen (Figure 4).

Figure 4. Login Screen

Once you install and launch the SRA Tool, you will notice four tabs on the right (Figure 5):

- Users – You may create new users on this tab

- About Your Practice – Enter information about your practice or business on this tab, including the name and contact information for your organization

- Business Associates – You may maintain a list of your business associates on this tab

- Asset Inventory" – You may maintain an inventory of your organization's IT assets on this tab

If this is the first time you have used the tool, navigate to the "Users" tab to begin.
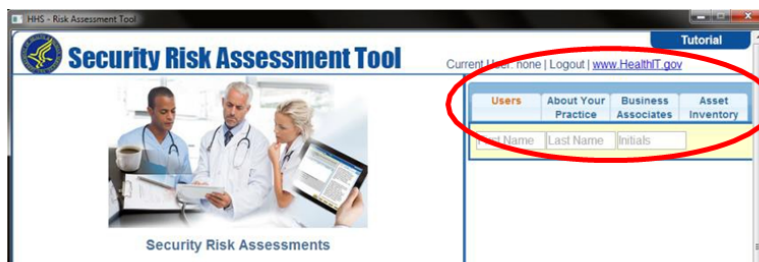

Figure 5. Login Screen Tabs

3.1.   Creating and Updating Users

To create a new user, type the user's first and last names and initials in the associated fields (Figure 6).

Figure 6. Creating a New User

Once you have entered the user's information, select the "Users" tab again to bring up the "Log In" button (Figure 7).
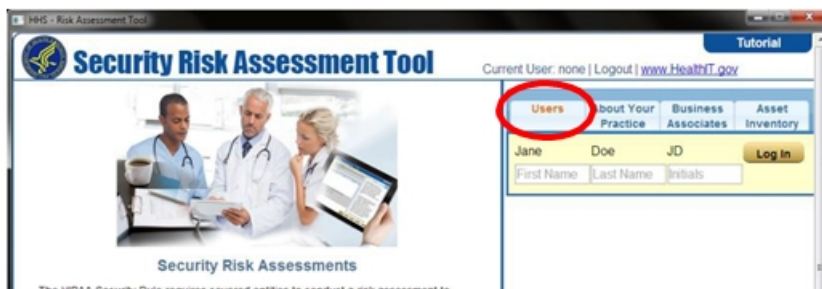

Figure 7. Saving Changes to a New User

If you have multiple users that will add information in the tool, you may want to create multiple users. The tool will track when a user makes an update to an assessment question; this will allow you to monitor who in your organization answered a specific question if you need to follow-up with them later. To add multiple users, simply type in their information using the additional fields. Each time you access the tool, all user names are pre-populated in the users list. When you log in again, you will already see your name listed, and can simply select the "Log In" button next to your credentials. Please remember that only one user can access the tool at any one time (Figure 8).

Figure 8. Editing a User

To edit a user, double-click on a user's name or initials. The selected field will become editable. When you have made the edits to the user, click "Finished" (Figure 9).

Figure 9. Saving Changes to an Edited User

To delete a user, double-click on a user's name or initials to begin editing that user. Then delete the user's first name, last name, and initials. Click "Finished" and the user will be deleted.

3.2. Adding Information About Your Practice

To add information about your practice or business such as your address, select the "About Your Practice" tab from the login screen (Figure 5). Fill in the "Name," "Address," "City," "State or Territory," "Zip Code," and "Telephone Number" in the corresponding fields (Figure 10). This information will be saved within the tool and will not be collected or maintained by HHS.
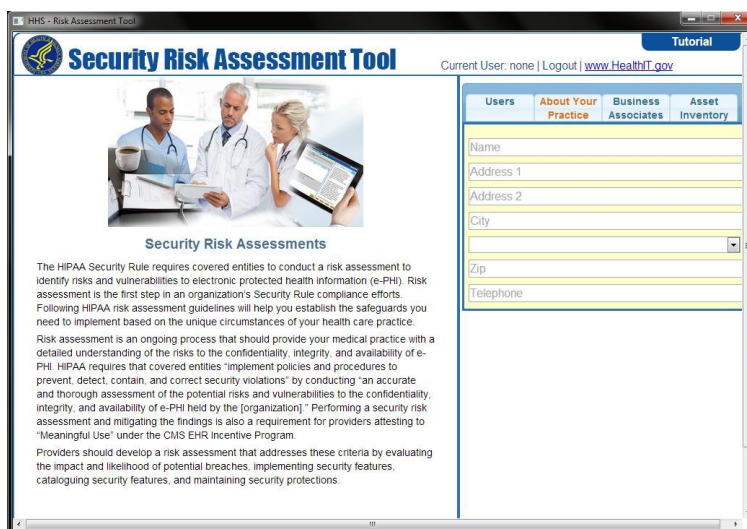

Figure 10. Filling out the About Your Practice Tab

3.3. Adding Information about Business Associates

To add information about your business associates, select the "Business Associates" tab from the login screen (Figure 5). You will need to fill in the "Name," "Type," and "Address" in the corresponding fields (Figure 11). There is no limit to the number of Business Associates you can add. New fields will be generated after you re-select the "Business Associates" header. For more information on who may be a Business Associate, please refer to the OCR website at: www.hhs.gov/ocr.

Figure 11. The Business Associate Tab

3.4.   Adding Information about IT Assets

To add information about IT assets, select the "Asset Inventory" tab from the login screen (Figure 5). Within this tab, you will see four fields, labeled "Name," "Type," "Has ePHI," and "Assignee." These fields have no field length. They will allow you to input as much information as needed (Figure 12).

Figure 12. The Assets Tab

Under "Name," provide the name for the information asset, for example, "Electronic Health Record (EHR)" or "Practice Management System." In the field labeled "Type," describe the type of asset. For example, you can label it "an application" and explain how ePHI is transmitted or stored. A copy machine may also store ePHI and therefore may be an example of an asset. The next field, labeled "Has ePHI," allows you to document if the asset receives, transmits, or stores ePHI. The last field, "Assignee," allows you to document who in your organization is responsible for this

particular asset.

3.5.   SRA Tool Login and Question Window

To log in, select the "Users" tab. Select the "Log In" button located next to your username on the login screen (Figure 4). After you log in, the first screen you will see explains the Administrative, Physical, and Technical Safeguards under the HIPAA Security Rule (Figure 13). Read the descriptions and disclaimer. In the lower right corner, you will see three options, "Import Assessment," "Create New," and "Continue Current."

- Import Assessment – Data can be exported from the SRA Tool into an SRA file. The SRA file can then be stored as an offline backup or transferred to another computer. An SRA file can be imported to another copy of the SRA Tool. This option allows you to import a previously exported SRA file. Importing and exporting SRA files is useful, for example, for transferring risk assessments between computers. For more information on importing or exporting SRA files, please see Section 3.10.

- Create New – This option allows you to create a brand new assessment. If this is your first time using the tool, this will be the only option to select. NOTE: If you already have data entered into the tool, selecting the "Create New" option will erase existing data in the tool.

- Continue Current – If you have previously imported an assessment or have already started an assessment, this option allows you to continue working on that assessment. NOTE: If you have previously entered data (even using a prior version of the tool), you should already have data the tool can access, so use this option if you want to add information to your previous assessment.

Figure 13. Administrative, Physical, and Technical Safeguards Screen

Once you select one of the three options, you will be placed on the SRA Tool Question Window (Figure 14)
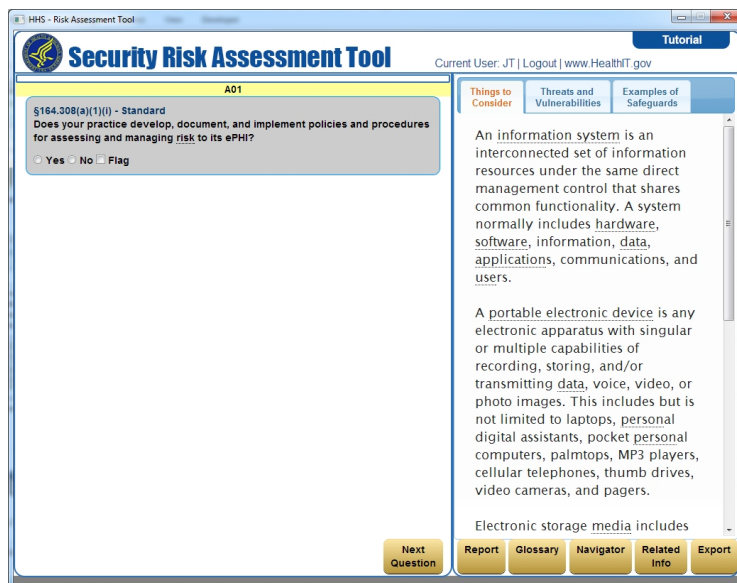
Figure 14. SRA Tool Question Window

The first question appears within the gray box on the left side of the tool. The question cites the Security Rule and displays if the item is "Standard," "Required," or "Addressable." Under the Security Rule, these terms are defined as:

- Standards – measures a covered entity must take ensure the confidentiality, integrity, and availability of ePHI while in the custody of covered entities and business associates as well as while in transit. Covered entities and business associates must comply with the applicable Standards provided in the Security Rule with respect to all ePHI.

- Implementation Specifications – may be either Required or Addressable. These are instructions for implementing Security Rule Standards.

- Required – Implementation Specifications must be implemented by the covered entity or business associate.

- Addressable – The concept of "addressable implementation specifications" was developed to provide covered entities additional flexibility with respect to compliance with the security standards. However, "addressable" does not mean "optional." For Implementation Specifications which are addressable, the covered entity or business associate must assess whether the implementation specification is a reasonable and appropriate security measure to apply when analyzed with reference to the likely contribution it would make to protecting ePHI in the organization's own environment. If it is, the entity must implement the specification; if not, the entity must document why it is not, and put in place alternative procedures (if reasonable and appropriate). For example, the **information access management standard** includes the addressable *Access Establishment and Modification implementation specification.* A solo practitioner with two employees may determine that it is not "reasonable and appropriate" to implement

14

policies and procedures to modify "…a user's right of access to a workstation, transaction, program or process" because all three workforce members require the same access to ePHI. The covered entity must document the rationale for deciding these particular measures were not reasonable and appropriate and what alternative measures are in place to comply with the Information Access Management standard.

If the implementation specification is reasonable and appropriate, then the covered entity or business associate must implement that addressable Implementation Specification.

If the implementation specification is determined to not be reasonable and appropriate, the covered entity or business associate must document why it would not be reasonable and appropriate and implement an equivalent alternative measure if reasonable and appropriate (see Appendix A Addressable and Required Specifications).

The yellow bar above each assessment question is labeled according to the type of Security Rule category the question covers. For example, "A" stands for "Administrative;" "T" for Technical; and "P-H" for "Physical." Questions are not in presented in numerical order. Instead, similar questions are grouped by topic across the administrative, technical, and physical sections.

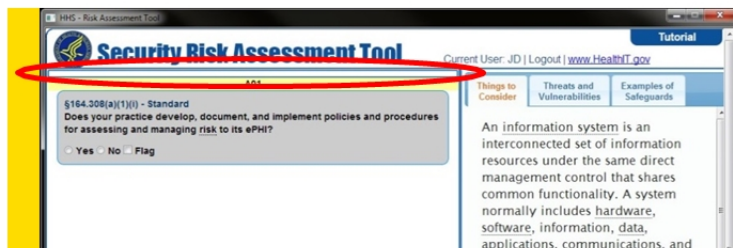Above the yellow bar is a progress bar to indicate how much of the assessment you have completed (Figure 15).

Figure 15. Progress Bar

At bottom right are five buttons that can help you use the tool (Figure 16):

- Report – This button creates a PDF or Microsoft Excel formatted report of the data you have entered into the SRA Tool. For more information on reporting, please see Section 3.7.

- Glossary – This button displays a glossary of frequently used terms in the SRA Tool

- Navigator – This button displays the "Navigator View." For more information on the Navigator View, please see Section 3.8.

- Related Info – This button displays the "Things to Consider," "Threats and Vulnerabilities," and "Examples of Safeguards" tabs. You may find these tabs useful when answering questions in the tool. For more information on the Related Info button, please see Section 3.6.

- Export – This button exports data in the tool into an SRA file. SRA files can be used to back up your risk assessment data, or to send to another user to open on their computer. For more information on exporting, please see Section 3.9.
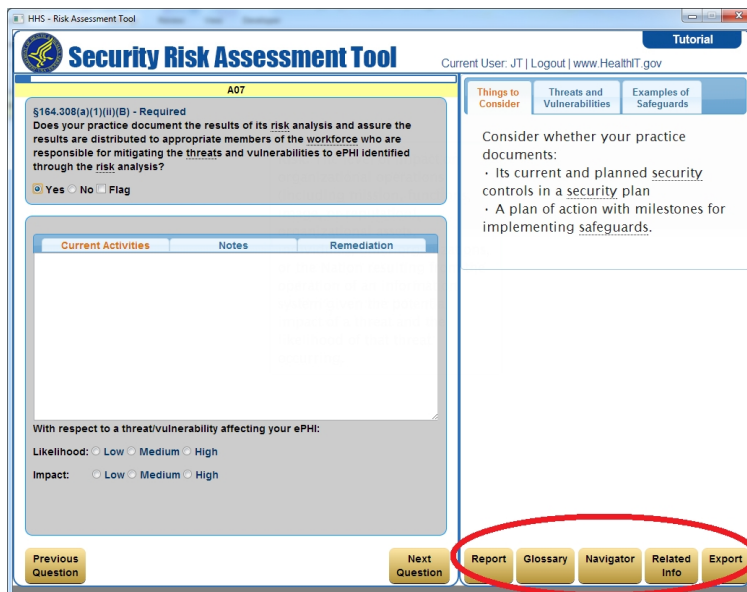
Figure 16. Navigation Buttons

3.6. Answering SRA Tool Questions

Once you have logged into the tool and are viewing the question window (see Section 3.5), you are now ready to answer the assessment questions in the tool. To answer a question, select either "Yes" or "No" below the question (Figure 17). You can also select the "Flag" option if you want to call attention to a question. Flagging can be done to remind you to review the question again later or to indicate to another person in your organization that you need them to review or answer the question.
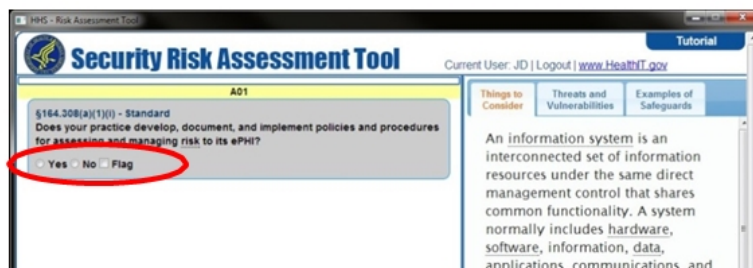

Figure 17. Answering a Question

If your answer is "No", then four radio buttons suggesting the best reason for answering "No" will be displayed: "Cost," "Practice Size," "Complexity," and "Alternate Solution" (Figure 18).
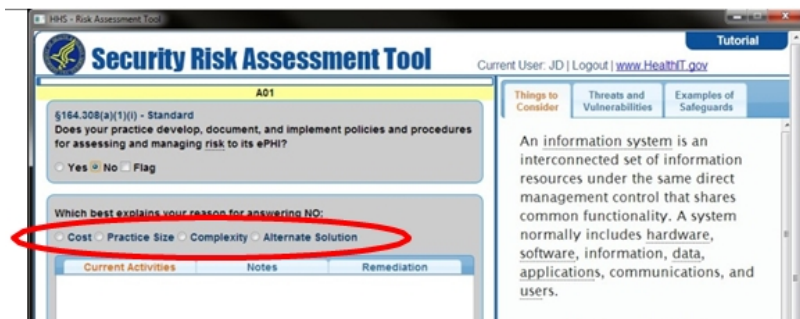
Figure 18. Reasons for Answering "No"

NOTE: If an implementation specification is described as "required," the specification must be implemented. Addressable means that if implementing the specification is not reasonable and appropriate, an alternative solution may be implemented that effectively safeguards the confidentiality, availability, and integrity of the protected health information (PHI). To better understand the elements of addressable specifications, see the Appendix on page 24.

Once you answer the assessment question (either "yes" or "no"), space is provided for you to: describe your current activities (i.e., what you are doing to meet the requirement), add any additional notes, or explain how you plan to address or remediate identified shortcomings (Figure 19). Select the appropriate tab for each category. The information you provide will appear in your risk assessment report.
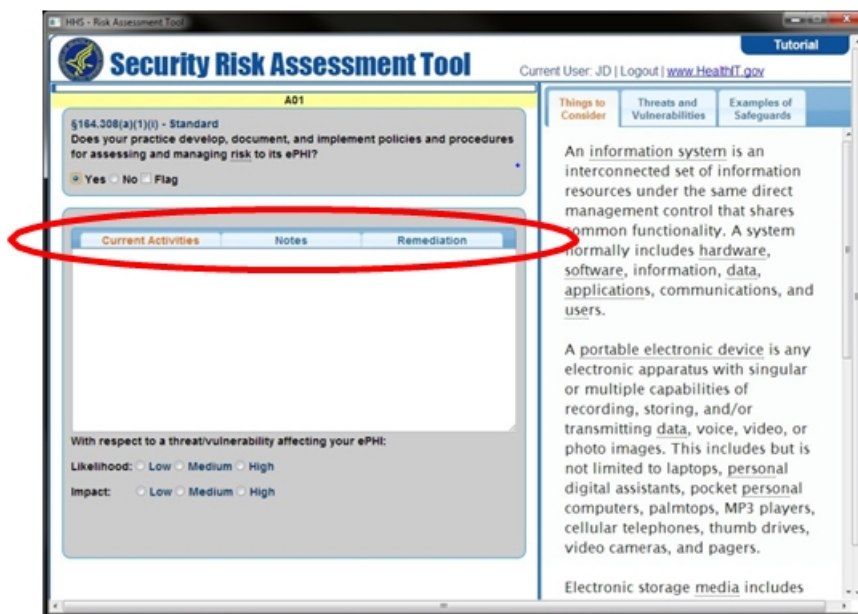

Figure 19. Current Activities, Notes, and Remediation Tabs

The radio buttons below the space allow you to document the likelihood that a particular threat could affect your ePHI. You can also rate the impact or level of harm that could occur if the standard or requirement stated in the question is not met (Figure 20).
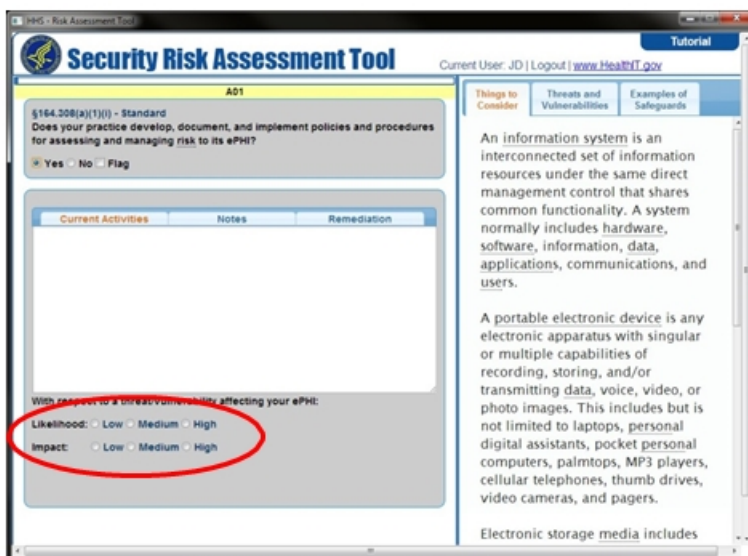
17

Figure 20. Risk Likelihood and Impact

On the right side of the question, there are three tabs that can help you understand and answer the question (Figure 21). "Things to Consider" gives you factors to think about when evaluating your practice. "Threats and Vulnerabilities" offers information to help you understand what some of the risks are and their potential impact. "Examples of Safeguards" provides some potential ways of reducing or eliminating risks or vulnerabilities. You may hover your mouse pointer over underlined words to view a tooltip bubble with the word's definition.
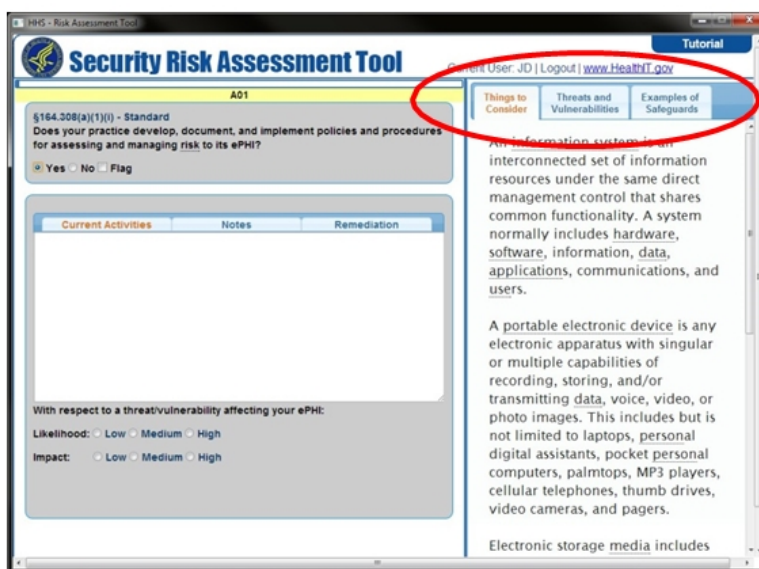

Figure 21. Things to Consider Tab

3.7.   Reporting

The "Report" button on the question window (Figure 16) opens up the Report Summary screen

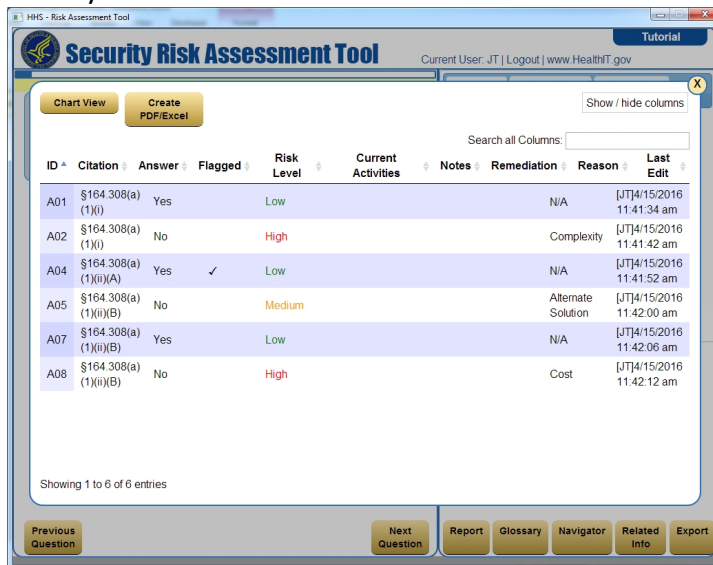(Figure 22). This screen lets you see the current status of the assessment results.

Figure 22. Report Summary Screen

The SRA Tool also provides options to create a portable document format (PDF) or Microsoft Excel document report of the data you have entered into the tool. To create a PDF or Excel report, select the "Create PDF/Excel" button on the Report Summary Screen. This will display the Report Options screen (Figure 23). On the Report Options screen, you may select:

- Report Format – Either PDF or Excel format

- Report Sections – Your responses to the SRA Tool questions are always included in the report. In addition, you may select that users, business associates, and your asset inventory are included in the report as well. Also, if you are generating a PDF report, you may choose to have the tool generate charts (Figure 26).

- Report Options – These options let you filter what information is produced in the report, such as the risk level, notes, citation, or last edit.
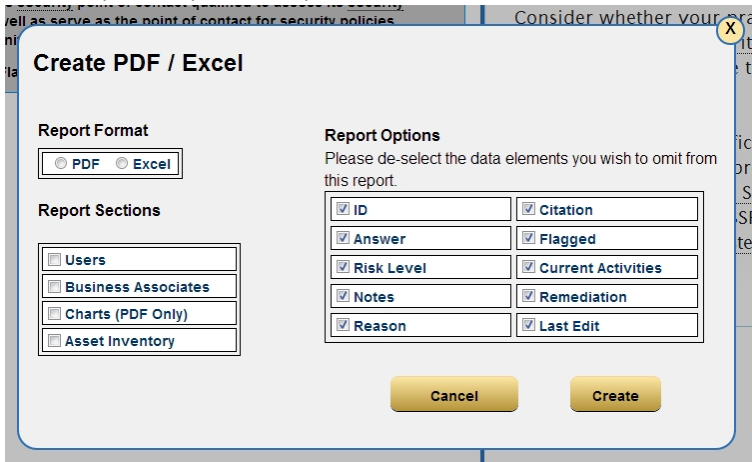

Figure 23. Report Options Screen

When you are finished selecting your report options, click on "Create" to create your PDF or Excel report. You will be prompted to select a location to save the report using a standard "Save As" dialog (Figure 24).
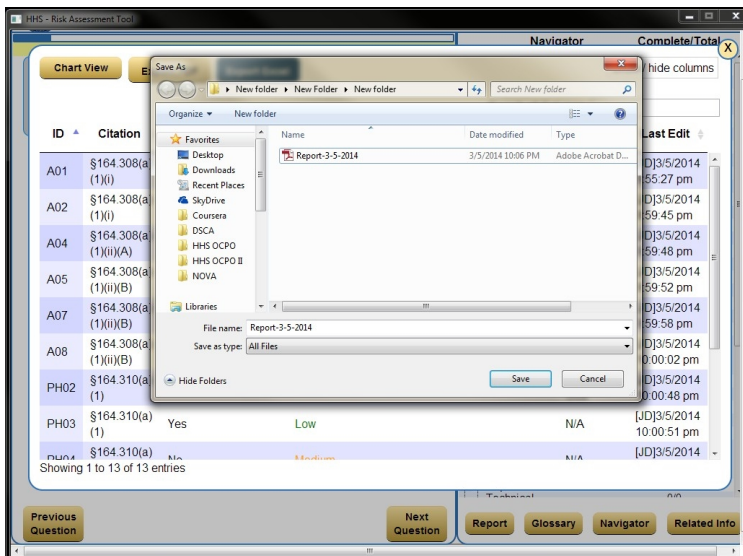

Figure 24. "Save As" Dialog for Report Creation

Once you select a file location to save the report, the tool will create your report. If you created a PDF report, the Report Preview Screen will pop-up (Figure 25). Within this window you will be able to scroll down to see the report. To close the pop-up window, simply click on the "X" button located at the top right of the window.
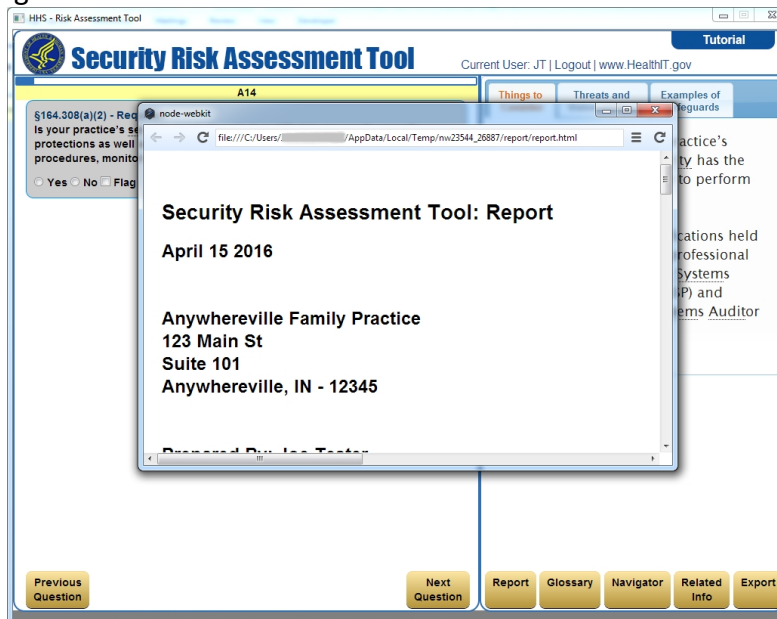

Figure 25. Report Preview Screen

To open the saved report, simply locate the file within the folder where you saved the report. NOTE: make sure to view your report before printing it. If you have selected a lot of columns, the

report may be very long or span many pages.

The report can also be viewed in a chart form (Figure 26). The chart can also be created in a PDF by selecting the "Charts" option on the Report Options Screen (Figure 23).

Figure 26. Chart Report

3.8.   Using the Navigator

The Navigator view allows you to both see how many questions are completed in each section and also navigate to a particular section at any time (Figure 27). This allows you to answer the questions in any order you desire. While you may answer questions in any order, the report will always display/print in the order of the HIPAA Security Rule. To access the Navigator view, click on the "Navigator" button on the SRA Tool question window (Figure 14).
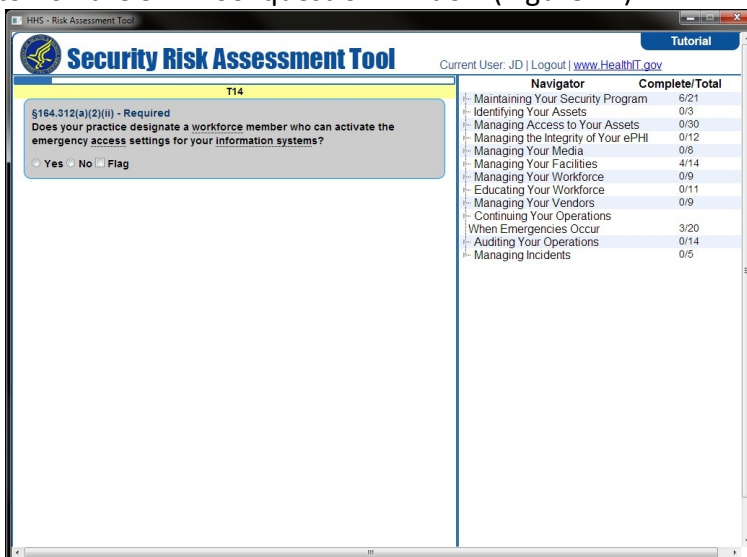

Figure 27. Navigator View

To move through the navigator sections, select the small grey arrow symbol and the question category will expand to display the Administrative, Physical and Technical sections (Figure 28). It will also indicate how many questions are in each section and how many of the questions have been answered.
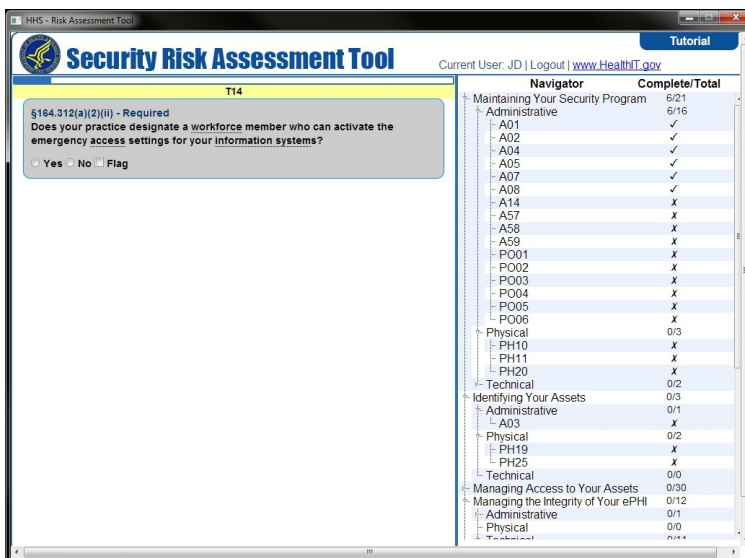

Figure 28. Expanded Navigator View

3.9.   Exporting Data from the SRA Tool

Data can be exported from the SRA Tool into an SRA file. The SRA file can then be stored as an offline backup or transferred to another computer. An SRA file can be imported to another copy of the SRA Tool. To export data, use the "Export" button located on the SRA Tool question window (Figure 14). When you click on the "Export" button, a standard "Save As" dialog will appear that allows you to select a location to save the SRA file (Figure 29).
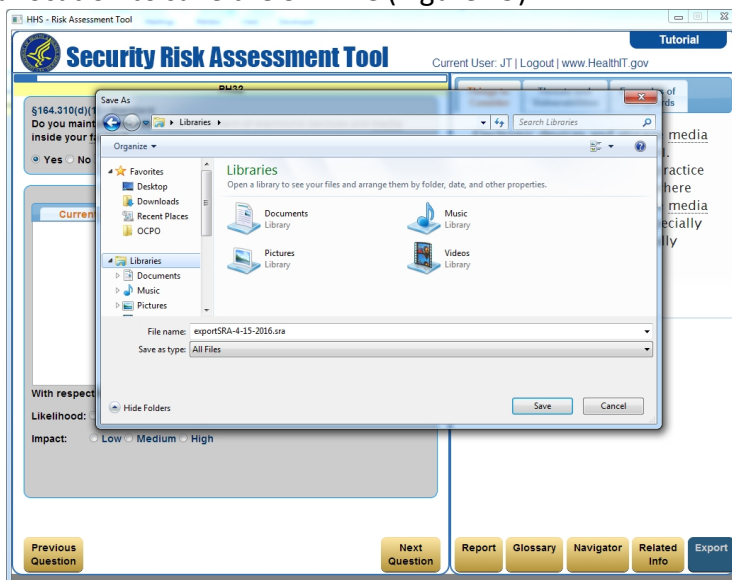

Figure 29. Exporting an SRA File

ONC strongly recommends that you regularly export data from the tool and save the exported SRA file as a backup of your security risk assessment. Ideally, backups should be stored in a separate location from the computer where the SRA Tool is installed. As exported SRA files are not encrypted, you should protect them with strong access controls or use your own encryption to protect the exported files.

If you have multiple facilities that require separate security risk assessments, you can use the export feature to work on multiple security risk assessments at a time.

3.10. Importing Data into the SRA Tool

If you have previously exported data from the SRA Tool, you can import the data from the Administrative, Physical, and Technical Safeguards screen (Figure 13). When you click the "Import" button, a standard system "Open" dialog will appear that allows you to select a previously exported SRA file. When you select a file, the data will be imported into the SRA Tool. **Please note, that importing an SRA file will overwrite any existing data in the tool.** If you do not want to lose existing data, be sure to export to a separate SRA file before you import a new one. For more on exporting SRA files, see Section 3.9.

3.11. Logging Out of the SRA Tool

To log out of the SRA Tool, select the "Logout" link located at the upper right of the SRA Tool question window (Figure 30). When you logout, all answers are stored for the next time you login. You can continue working on your assessment by clicking the "Continue Current" button on the Administrative, Physical, and Technical Safeguards screen (Figure 13).
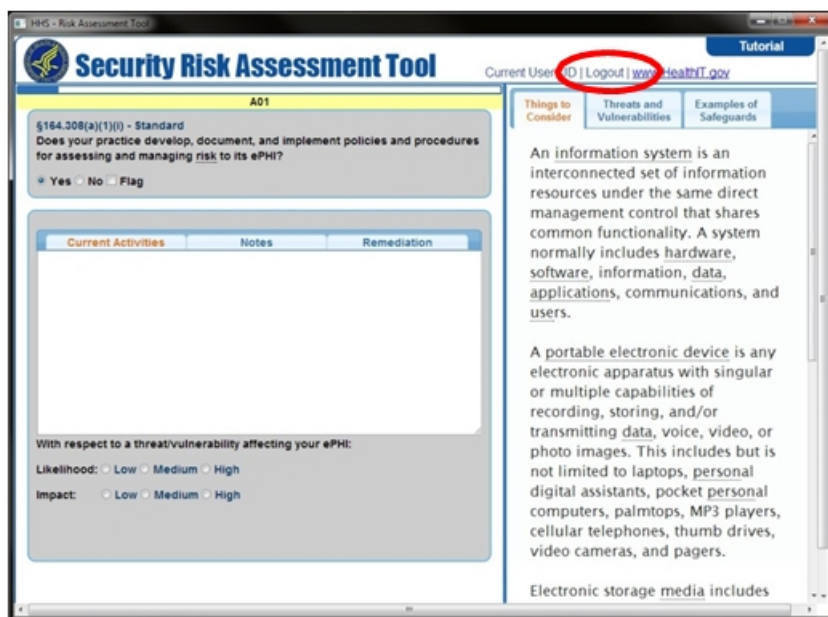

Figure 30. SRA Tool Logout Button

4. Uninstalling the SRA Tool

To uninstall the SRA Tool, first remove any data cached in the tool. To do this, login to the tool and select "Create New" from the Administrative, Physical, and Technical Safeguards screen (Figure 13). This will remove any data that is cached in the tool. Next, you may delete the SRA Tool program that you downloaded to your computer. This uninstalls the application.

Appendix A. Addressable and Required Specifications

In meeting standards that contain addressable implementation specifications, a covered entity must do one of the following for each addressable specification:

(a) implement the addressable implementation specification;
(b) implement one or more alternative security measures to accomplish the same purpose; or
(c) not implement either an addressable implementation specification or an alternative.

However, in all cases, the covered entity or business associate must meet the standard.

The covered entity's choice must be documented. The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. A covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative.

This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a covered entity makes regarding addressable specifications must be documented. Users may use the space provided in the SRA tool and the radio buttons to document how the organization will implement addressable specifications. More information is available from: http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2020.html