

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 Date: March 2014

DISCLAIMER

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

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

Contents

Contents	ii
Acronym Index	iii
1.0 Introduction.....	1
1.1 Purpose	1
1.2 Audience.....	1
1.3 What the SRA Tool Is	1
1.4 The Role of the SRA Tool in a Risk Assessment	2
1.5 What the SRA Tool Is Not	2
2.0 Using the SRA Tool.....	2
2.1 Downloading the SRA Tool (Windows version)	2
2.2 Downloading the SRA Tool (iPad version)	5
2.3 Using the SRA Tool	6
2.4 Logging out of the SRA Tool.....	22
2.5 Clearing stored data on the SRA Tool (Windows 7 version).....	23
3.0 Appendix A.....	26

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
IP	Internet Protocol
NIST	National Institute of Standards and Technology
OCR	The Office for Civil Rights
ONC	The Office of the National Coordinator for Health Information Technology
OS	Operating System
PDF	Portable Document Format
PHI	Protected Health Information
SRA Tool	Security Risk Assessment Tool



1.0 Introduction

Welcome to the Security Risk Assessment Tool (SRA Tool), designed to help healthcare practices to evaluate risks, vulnerabilities and adherence to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. We hope you find this tool helpful as you work towards improving the privacy and security of your healthcare 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, and therefore is only as useful as the work that goes into performing and recording the risk assessment process. Use of this tool does not mean that your practice is compliant with the HIPAA Security Rules or other federal, state or local laws and regulations.

1.1 Purpose

The purpose of the SRA Tool is to assist healthcare practices in performing and documenting a Security Risk Assessment. The HIPAA Security Rule, effective since 2005, requires that all healthcare organizations that are covered entities or business associates under the HIPAA Privacy and Security Rules conduct a thorough and accurate Risk 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 healthcare 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. For the purposes of grant funding and technical assistance, The Office of the National Coordinator for Health Information Technology (ONC) has historically defined small to medium sized practices to be those with one to ten healthcare providers. This SRA Tool was designed to assist these smaller organizations in performing and documenting a risk assessment.

1.3 What the SRA Tool Is

The SRA Tool is a software application that is intended to be a useful resource (among other tools and processes) that a healthcare practice can use to assist in reviewing its implementation of the HIPAA Security Rule. It is a self-contained, operating system (OS) independent application that can be run on various environments including Windows 7 OS for desktop and laptop computers and Apple's iOS for iPad. The iOS SRA Tool application for iPad, available at no cost, can be downloaded from Apple's App Store (see section 2.2 downloading the SRA Tool (Mobile version) for instructions on how to download.)

The SRA Tool addresses the 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, backups, recoveries, and technical and physical security. Risk management questions address periodic reviews and evaluations and can include regular functions, such as continuous monitoring.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management.



Lastly, personnel issue questions address access to information as well as the on-boarding and release of staff.

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

- HIPAA Security Rule
- National Institute of Standards and Technology (NIST) Special Publication 800-66*
- NIST Special Publication 800-53*
- NIST Special Publication 800-53A*
- Health Information Technology for Economic and Clinical Health (HITECH) Act

1.4 The Role of the SRA Tool in a Risk Assessment

The use of the SRA Tool can support an organization's risk assessment process. The purpose of a risk assessment is to identify conditions where Electronic Protected Health Information (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 designed to protect ePHI may need to be implemented or where existing implementations may need to be improved.

1.5 What the SRA Tool Is Not

A Multi-User Tool. The SRA Tool is not intended to be, nor was it built to be, a collaborative multi-user 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 desktop will use the tool to individually capture information. However, multiple users may access the tool on separate occasions.

A Compliance Tool. The SRA Tool does not produce a statement of compliance. Organizations may use the SRA Tool in coordination with other tools and processes to support HIPAA Security Rule – Risk Analysis compliance and risk management activities. Statements of compliance are the responsibility of the covered entity and the HIPAA Security Rule regulatory and enforcement authority. Please note that the SRA Tool does not cover additional Security Rule requirements.

A HIPAA Privacy Rule Tool. The SRA Tool provides guidance in understanding the requirements of the HIPAA Security Rule – Risk Analysis specifically, and does not include provisions for the HIPAA Privacy Rule.

2.0 Using the SRA Tool

2.1 Downloading the SRA Tool (Windows version)

To download the SRA Tool, navigate to ONC's website at: <http://www.healthit.gov/security-risk-assessment>

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management.



Figure 1

Next, select the blue button located within the “Security Risk Assessment Tool” box.



Figure 2

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.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.



Figure 3

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.



Figure 4

From the menu options, select “Save As” then select the folder location where you would like to store your application. Finally, select the “Save” button.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

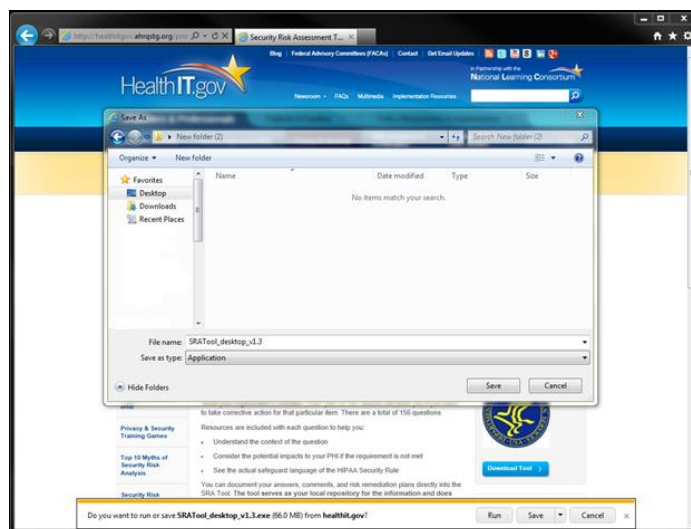


Figure 5

Once you have downloaded the file, you should save the file to a folder that can be password protected and encrypted. While the SRA tool does not ask for any patient health information, using the tool will document the risks and vulnerabilities in your healthcare practice, and therefore should be safeguarded. **You can better secure the tool by password protecting or encrypting the folder where it will be stored, as the tool itself is not encrypted or password protected.**

2.2 Downloading the SRA Tool (iPad version)

To download the free SRA Tool onto your iPad, you will need to access Apple's App Store. Since there is no iPhone SRA Tool application, you will only see it available for the iPad.

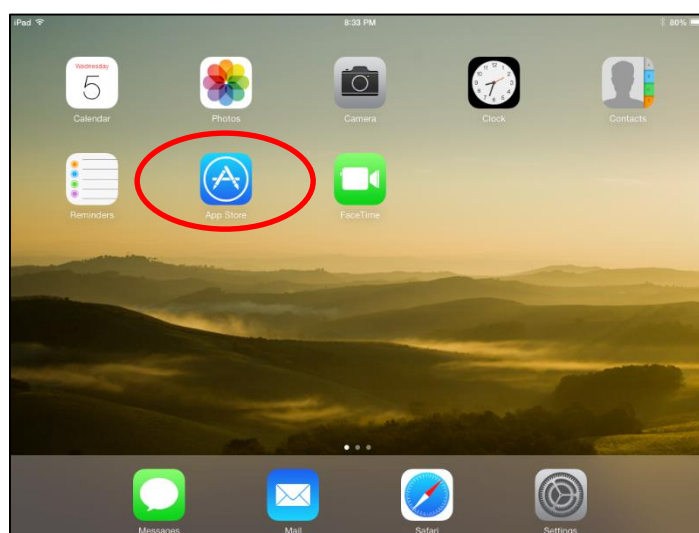


Figure 6

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management.

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.

2.3 Using the SRA Tool

Once you have downloaded the application and either saved it to your computer, a shared server, or in the case of iPad users, downloaded it to your device.

Double-click the icon and select “run” when prompted. The SRA Tool will open.



Figure 7

Once you install and launch the SRA Tool, you will notice four tabs on the right — “Users,” “About Your Practice,” “Business Associates,” and “Asset Inventory.”

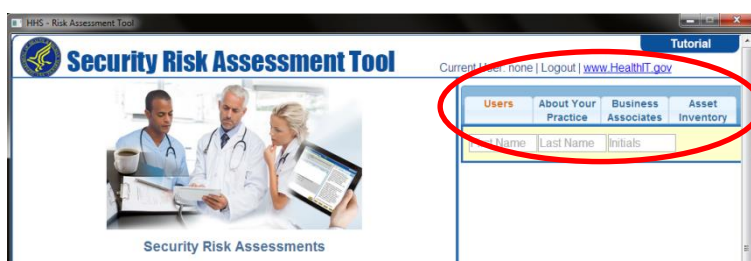


Figure 8

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

If this is the first time you have used the tool, navigate to the “Users” tab to begin. Type your first and last names and your initials in the associated fields.



Figure 9

Once you have entered your information, select the “Users” tab again to bring up the “Log In” button.

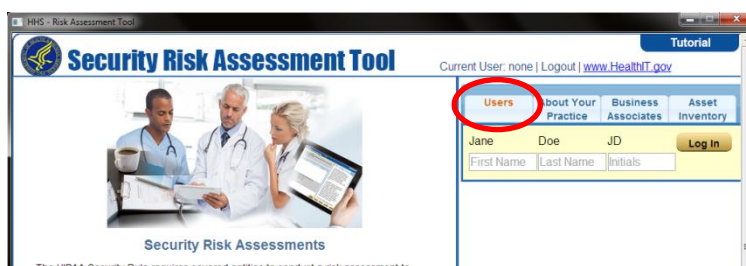


Figure 10

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 11

Next, select the “About Your Practice” tab. You will only need to enter your practice’s information once. Fill in the “Name,” “Address,” “City,” “State or Territory,” “Zip Code,” and “Telephone Number” in the corresponding fields. This information will be saved within the tool and will not be collected or maintained by HHS. You will see it the next time you log in.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.



Security Risk Assessment Tool

Current User: none | Logout | www.HealthIT.gov

Users | **About Your Practice** | **Business Associates** | **Asset Inventory**

Name:

Address 1:

Address 2:

City:

Zip:

Telephone:

Security Risk Assessments

The HIPAA Security Rule requires covered entities to conduct a risk assessment to identify risks and vulnerabilities to electronic protected health information (e-PHI). Risk assessment is the first step in an organization's Security Rule compliance efforts. Following HIPAA risk assessment guidelines will help you establish the safeguards you need to implement based on the unique circumstances of your health care practice.

Risk assessment is an ongoing process that should provide your medical practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI. HIPAA requires that covered entities "implement policies and procedures to prevent, detect, contain, and correct security violations" by conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the [organization]." Performing a security risk assessment and mitigating the findings is also a requirement for providers attesting to "Meaningful Use" under the CMS EHR Incentive Program.

Providers should develop a risk assessment that addresses these criteria by evaluating the impact and likelihood of potential breaches, implementing security features, cataloguing security features, and maintaining security protections.

Figure 12

After you complete the "About Your Practice" section, select the "Business Associates" tab. You will need to fill in the "Name," "Type," and "Address" in the corresponding fields. 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 Office for Civil Rights (OCR) website at: www.hhs.gov/ocr



Security Risk Assessment Tool

Current User: none | Logout | www.HealthIT.gov

Users | **About Your Practice** | **Business Associates** | **Asset Inventory**

Name: Type: Address:

Security Risk Assessments

The HIPAA Security Rule requires covered entities to conduct a risk assessment to identify risks and vulnerabilities to electronic protected health information (e-PHI). Risk assessment is the first step in an organization's Security Rule compliance efforts. Following HIPAA risk assessment guidelines will help you establish the safeguards you need to implement based on the unique circumstances of your health care practice.

Risk assessment is an ongoing process that should provide your medical practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI. HIPAA requires that covered entities "implement policies and procedures to prevent, detect, contain, and correct security violations" by conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the [organization]." Performing a security risk assessment and mitigating the findings is also a requirement for providers attesting to "Meaningful Use" under the CMS EHR Incentive Program.

Providers should develop a risk assessment that addresses these criteria by evaluating the impact and likelihood of potential breaches, implementing security features, cataloguing security features, and maintaining security protections.

Figure 13

Finally, select the "Asset Inventory" tab. Within this tab, you will see four fields, labeled "Name," "Type," "Has EPHI," and "Assignee." These fields will allow you to input as much information as needed.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management.



Figure 14

Under “Name,” provide the name for the information asset, such as “Electronic Health Record (EHR)” or “Practice Management System,” for example.



Figure 15

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.



Figure 16

The next field, labeled “Has EPHI,” allows you to document if the asset receives, transmits, or stores EPHI.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.



Figure 17

The last field, “Assignee,” allows you to document who in your organization is responsible for this particular asset.



Figure 18

Once you complete all four tabs, your information will be saved in the tool and available every time you log in. To log in, select the “Users” tab. Select the “Log In” button located next to your user credentials.

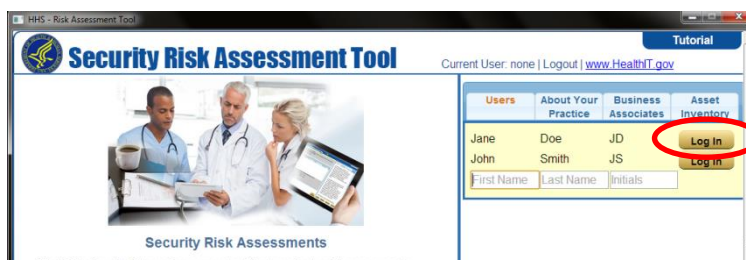


Figure 19

After you log in, the first screen you will see explains the Administrative, Physical, and Technical Safeguards under the HIPAA Security Rule. Once you have read the descriptions and disclaimer, select the “Start Assessment” button in the lower right corner.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

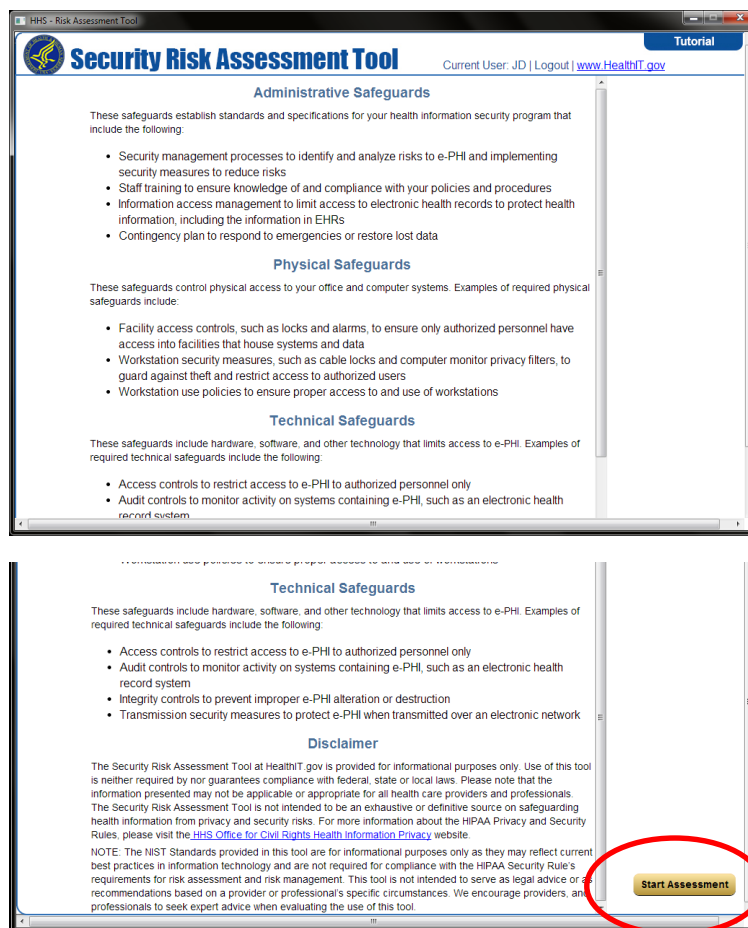


Figure 20

Once you click on “Start Assessment” you will be shown the first question in the risk assessment.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management.

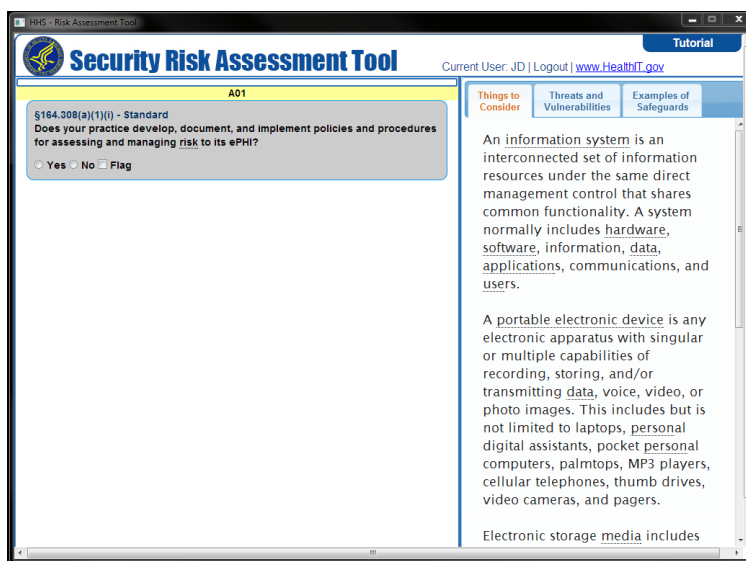


Figure 21

You may log in and out of the SRA tool multiple times and your information will always be saved.

When you log in to the SRA Tool, you will always be taken to the first question, although you will be able to navigate to the last question you entered by using the “Navigator” feature (see page 19 for more information on how to use the Navigator button).

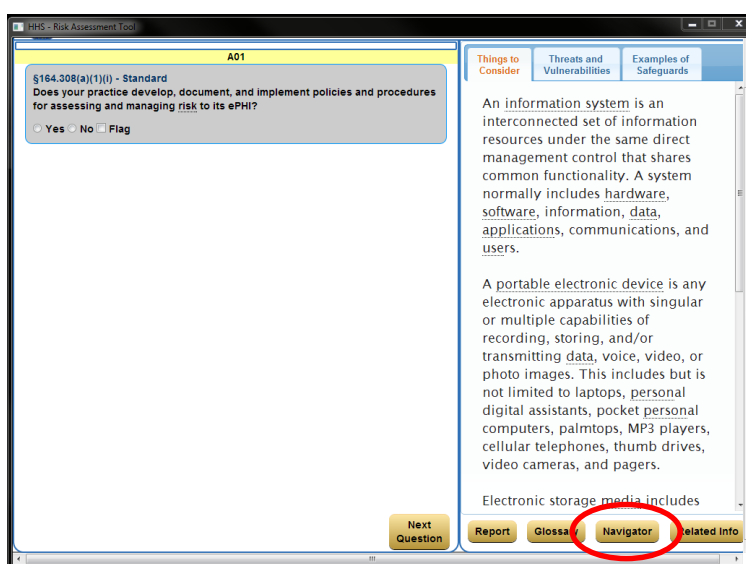


Figure 22

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.”

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

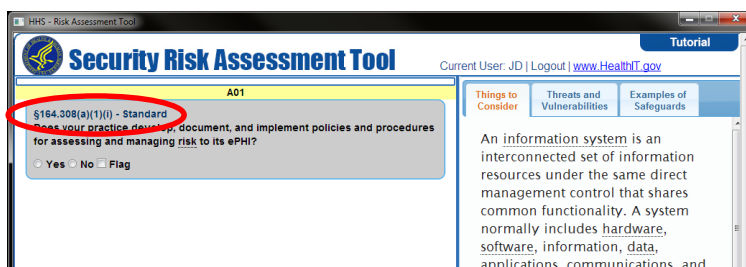


Figure 23

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.” While each question has a number, the questions are not in numerical order. Instead, similar questions are grouped together across the administrative, technical, and physical sections.

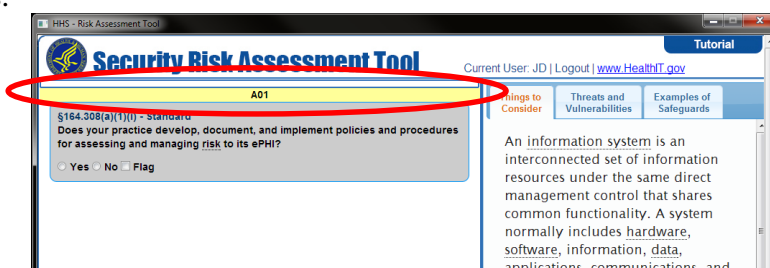


Figure 24

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

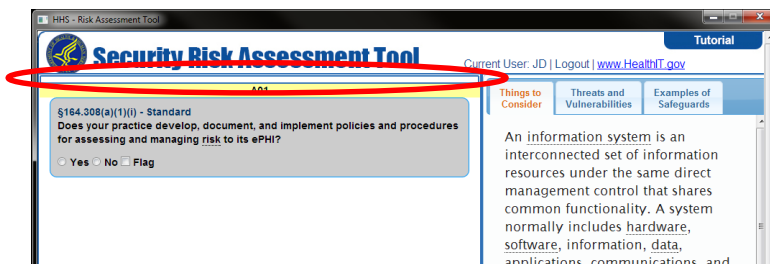


Figure 25

When you are ready to answer the assessment question, select either “Yes” or “No” below the question. 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.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

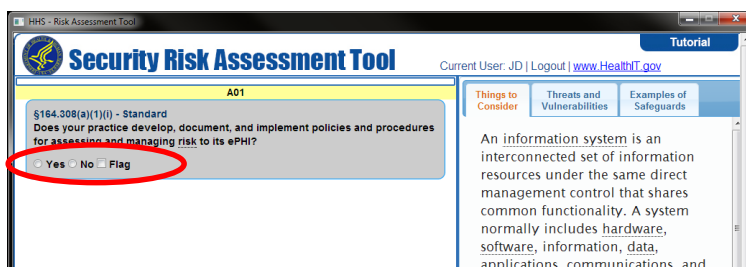


Figure 26

If your answer is “No”, only then will four radio buttons suggesting the best reason for answering no will be displayed, “Cost,” “Practice Size,” “Complexity,” and “Alternate Solution.” As stated previously, each question is labeled Standard, Required or Addressable.

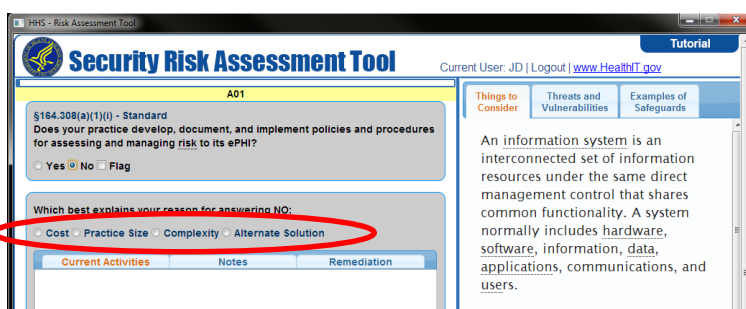
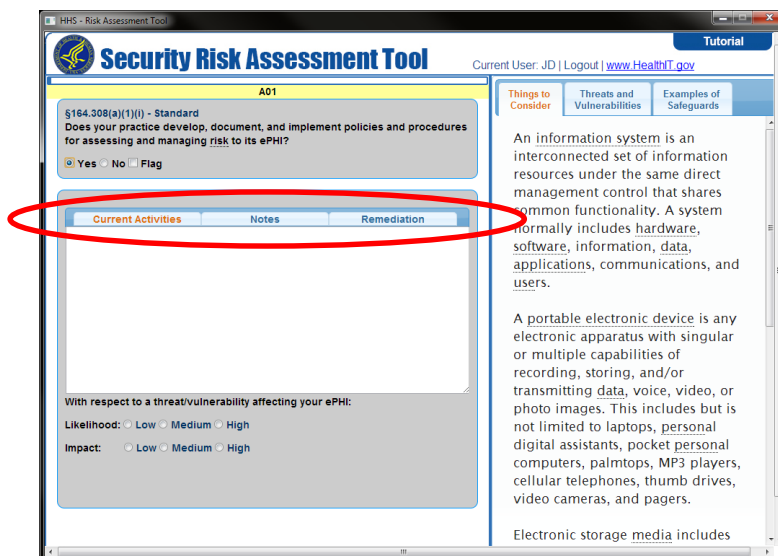


Figure 27

NOTE: If an implementation specification is described as “required,” the specification must be implemented. 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”. Rather addressable means that an alternative solution may be implemented if it would also effectively safeguard the confidentiality, availability and integrity of the protected health information (PHI). To better understand the elements of addressable specifications, see Appendix page 24.

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

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.



HHHS - Risk Assessment Tool

Security Risk Assessment Tool

Current User: JD | Logout | www.HealthIT.gov

A01

§164.308(a)(1)(i) - Standard
Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?

☒ Yes ☐ No ☐ Flag

Current Activities | Notes | Remediation

With respect to a threat/vulnerability affecting your ePHI:

Likelihood: ☐ Low ☐ Medium ☐ High

Impact: ☐ Low ☐ Medium ☐ High

Things to Consider | Threats and Vulnerabilities | Examples of Safeguards

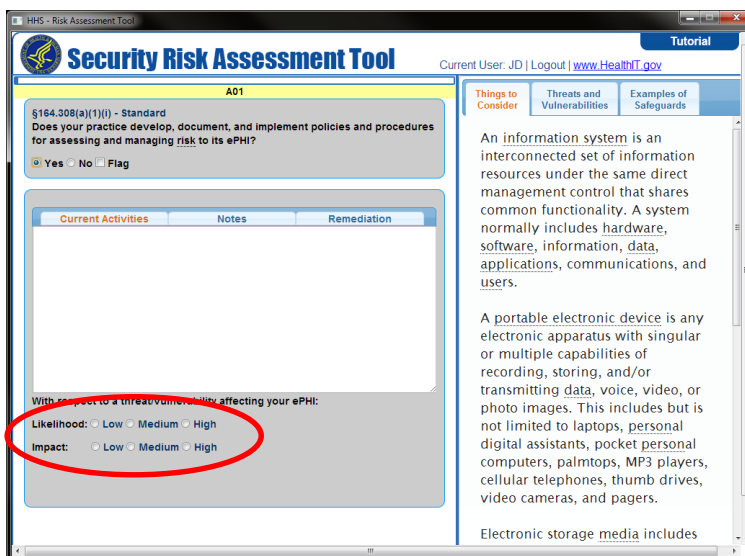
An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.

A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Electronic storage media includes

Figure 28

The radio buttons below the space allow you to judge 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



HHHS - Risk Assessment Tool

Security Risk Assessment Tool

Current User: JD | Logout | www.HealthIT.gov

A01

§164.308(a)(1)(i) - Standard
Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?

☒ Yes ☐ No ☐ Flag

Current Activities | Notes | Remediation

With respect to a threat/vulnerability affecting your ePHI:

Likelihood: ☐ Low ☐ Medium ☐ High

Impact: ☐ Low ☐ Medium ☐ High

Things to Consider | Threats and Vulnerabilities | Examples of Safeguards

An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.

A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Electronic storage media includes

Figure 29

On the right side of the question, there are three tabs that can help you understand and answer the question. “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.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.



Figure 30

At bottom right are four buttons that can help you use the tool.

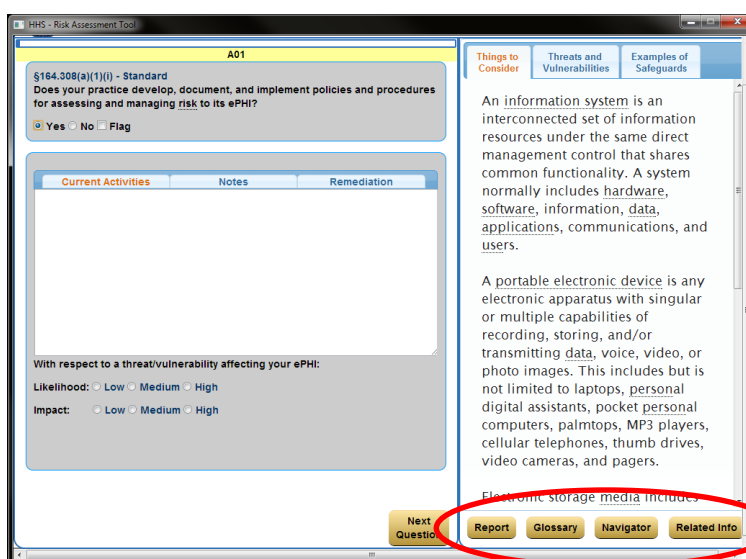
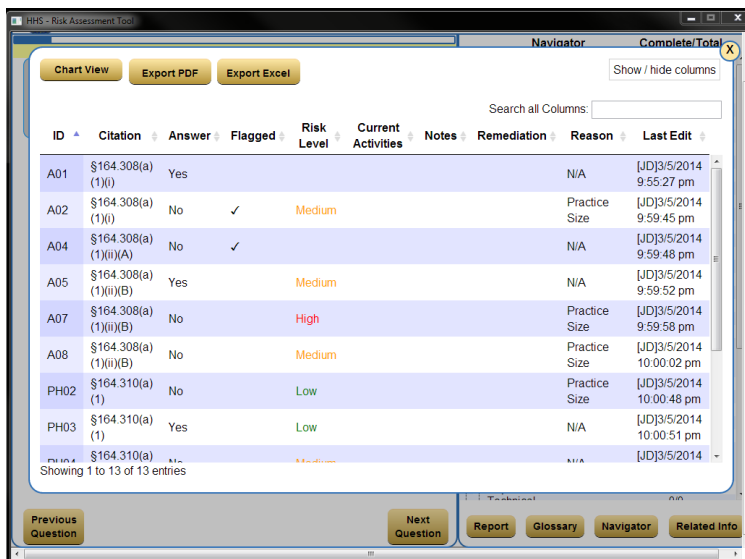


Figure 31

The “Report” button lets you see the current status of the assessment results.

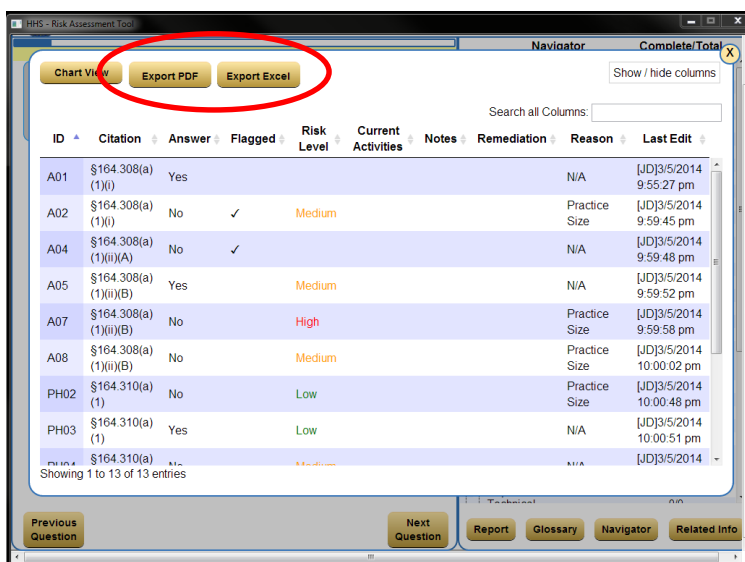
*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.



ID	Citation	Answer	Flagged	Risk Level	Current Activities	Notes	Remediation	Reason	Last Edit
A01	\$164.308(a)(1)(i)	Yes						N/A	[JD]3/5/2014 9:55:27 pm
A02	\$164.308(a)(1)(i)	No	✓	Medium				Practice Size	[JD]3/5/2014 9:59:45 pm
A04	\$164.308(a)(1)(ii)(A)	No	✓					N/A	[JD]3/5/2014 9:59:48 pm
A05	\$164.308(a)(1)(ii)(B)	Yes		Medium				N/A	[JD]3/5/2014 9:59:52 pm
A07	\$164.308(a)(1)(ii)(B)	No		High				Practice Size	[JD]3/5/2014 9:59:58 pm
A08	\$164.308(a)(1)(ii)(B)	No		Medium				Practice Size	[JD]3/5/2014 10:00:02 pm
PH02	\$164.310(a)(1)	No		Low				Practice Size	[JD]3/5/2014 10:00:48 pm
PH03	\$164.310(a)(1)	Yes		Low				N/A	[JD]3/5/2014 10:00:51 pm
PH04	\$164.310(a)(1)							N/A	[JD]3/5/2014

Figure 32

The report can also be exported as a portable document format (PDF) or Excel document.



ID	Citation	Answer	Flagged	Risk Level	Current Activities	Notes	Remediation	Reason	Last Edit
A01	\$164.308(a)(1)(i)	Yes						N/A	[JD]3/5/2014 9:55:27 pm
A02	\$164.308(a)(1)(i)	No	✓	Medium				Practice Size	[JD]3/5/2014 9:59:45 pm
A04	\$164.308(a)(1)(ii)(A)	No	✓					N/A	[JD]3/5/2014 9:59:48 pm
A05	\$164.308(a)(1)(ii)(B)	Yes		Medium				N/A	[JD]3/5/2014 9:59:52 pm
A07	\$164.308(a)(1)(ii)(B)	No		High				Practice Size	[JD]3/5/2014 9:59:58 pm
A08	\$164.308(a)(1)(ii)(B)	No		Medium				Practice Size	[JD]3/5/2014 10:00:02 pm
PH02	\$164.310(a)(1)	No		Low				Practice Size	[JD]3/5/2014 10:00:48 pm
PH03	\$164.310(a)(1)	Yes		Low				N/A	[JD]3/5/2014 10:00:51 pm
PH04	\$164.310(a)(1)							N/A	[JD]3/5/2014

Figure 33

To export as a PDF simply select the “Export PDF” button located at the top. Choose the desired location (folder) to save the report and select the “Save” button. You can also rename your report within the “File Name” field before selecting the “Save” button. To open the saved PDF file, simply locate the file within the folder where you saved the report.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

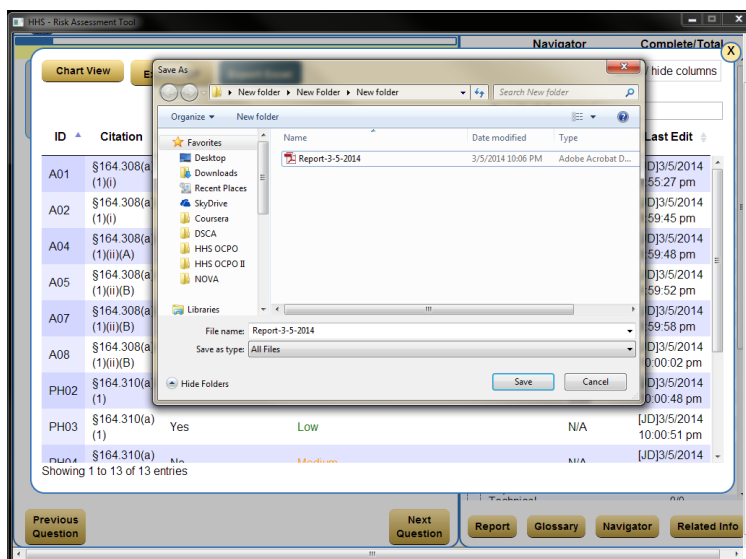


Figure 34

Once you select the “Save” button, the “Node-webkit” pop-up window will display. Within this window you will be able to scroll down to see the report as it will be saved and printed from the PDF file. To close the pop-up window, simply click on the “X” button located at the very top of the window.

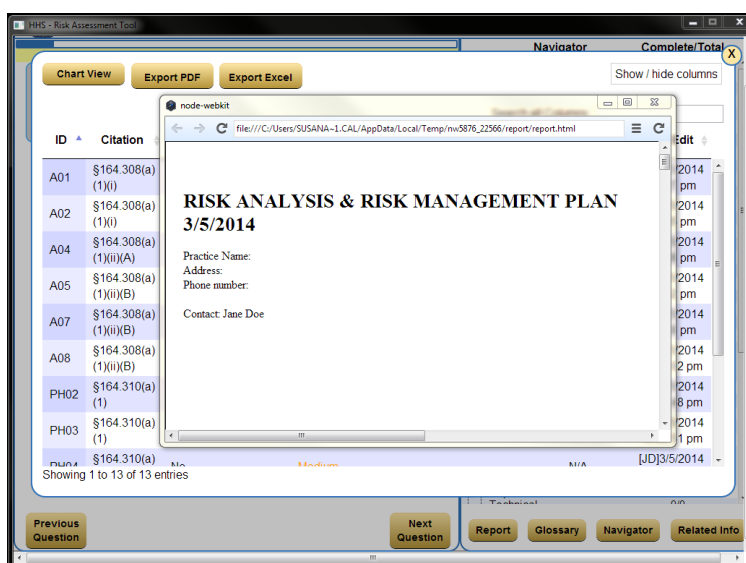


Figure 35

To export the report as an Excel file, simply select the “Export Excel” button located at the top. Choose the desired location (folder) to save the report and select the “Save” button. You can also rename your report within the “File Name” field before selecting the “Save” button. To open the saved Excel file, simply locate the file within the folder where you saved the report. Once you

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

select the “Save” button, the Save As window will disappear and the “Node-webkit” will not display. The “Node-webkit” only displays when the report is exported as a PDF.

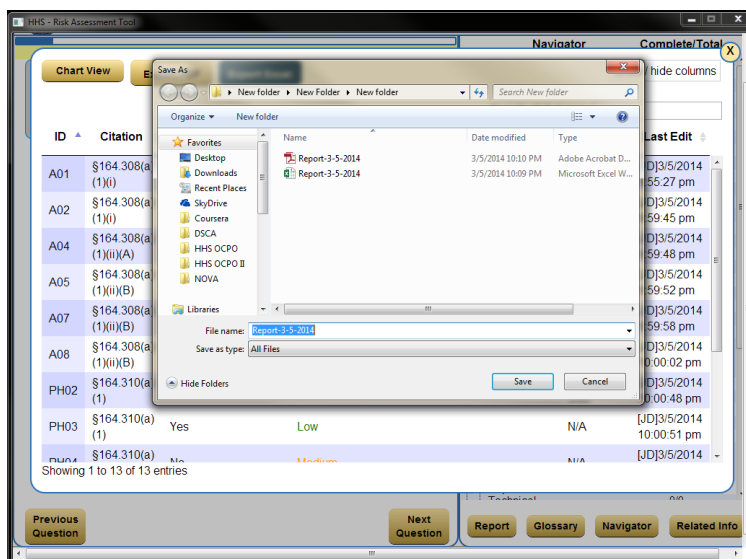


Figure 36

The report can also be viewed in a colorful chart form. Reports can be accessed at any time, even before the assessment is complete.



Figure 37

The “Glossary” button allows you to search for definitions of words. You can scroll through the glossary, sort by a column or use the search box to quickly find a glossary term. Also, note that the “X” in the upper right corner allows you to exit the report and or the glossary.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

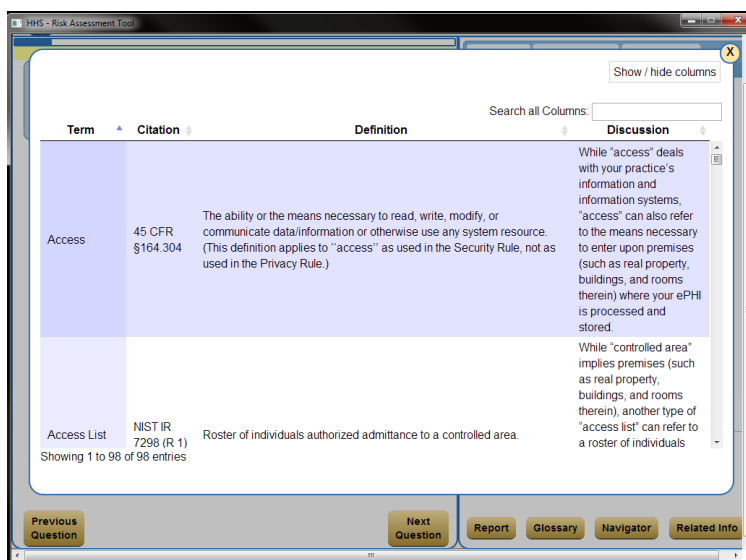


Figure 38

Words that are underlined throughout the tool can also be found within the glossary.

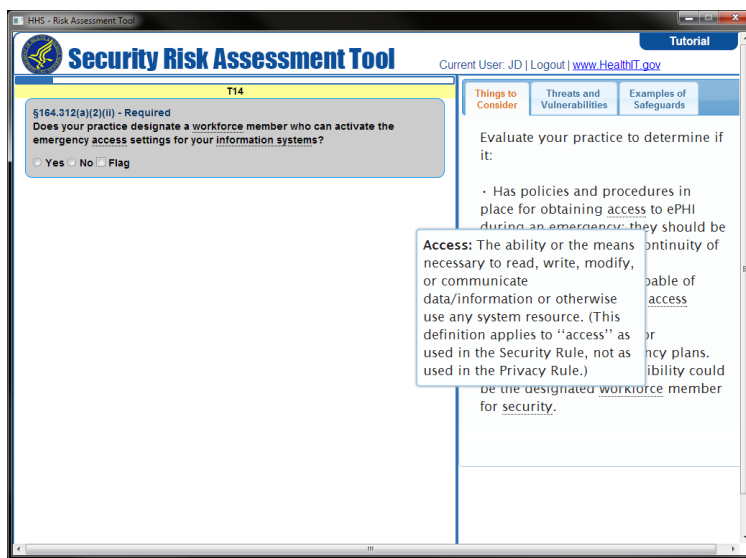


Figure 39

The "Navigator" button allows you to both see how many questions are completed in each section and also jump to a particular section at any time. 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.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management.

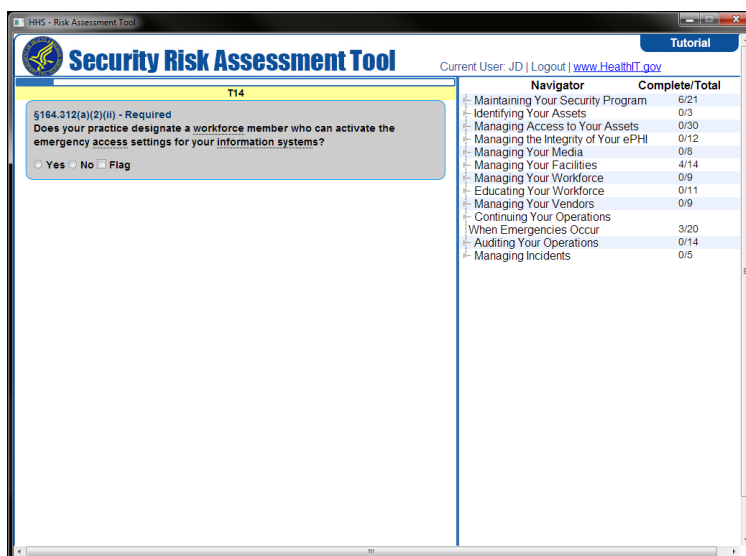


Figure 40

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. It will also indicate how many questions are in each section and how many of the questions have been answered.

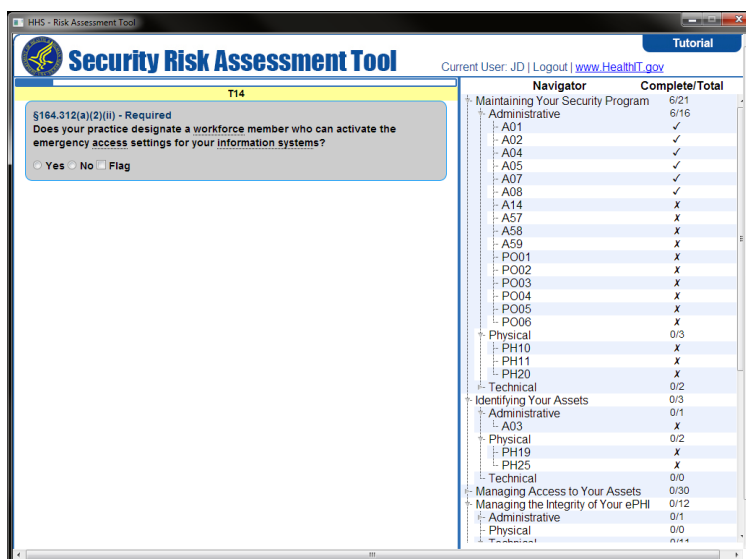


Figure 41

The “Related Info” button calls up the “Things to Consider,” “Threats and Vulnerabilities,” and “Examples of Safeguards” tabs.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

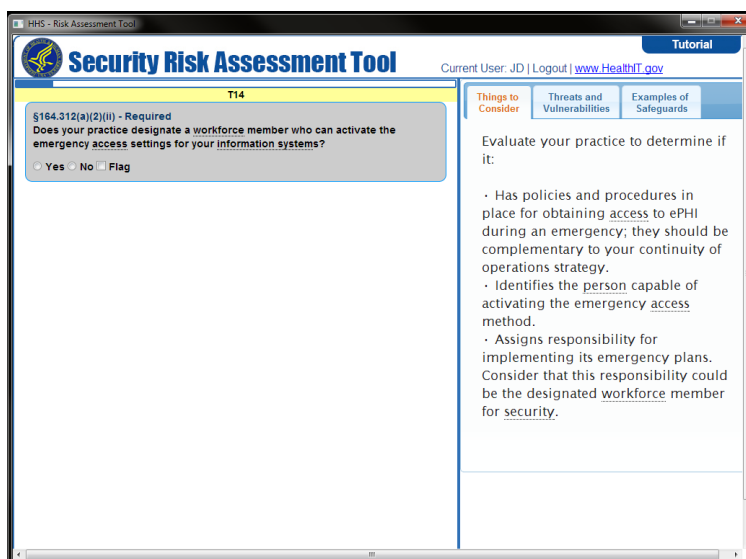


Figure 42

2.4 Logging out of the SRA Tool

Once you are ready to end your session or simply take a break, you can log out of the tool. To log out, select the “Logout” link located at the upper right of the tool.

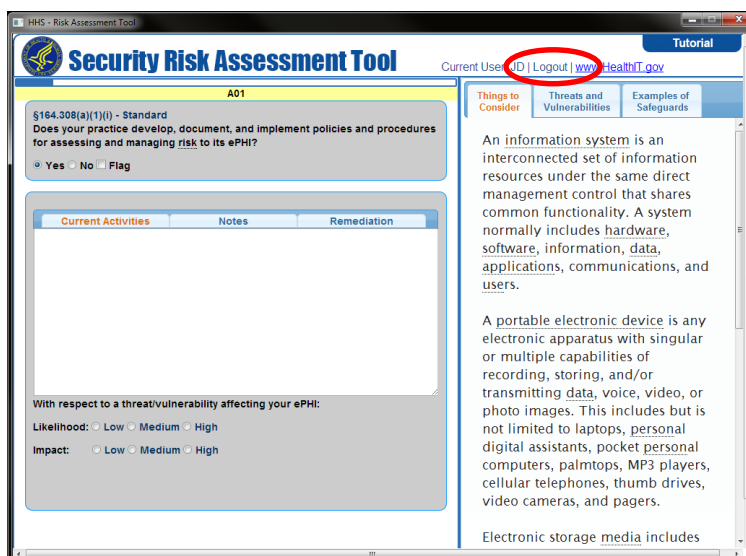
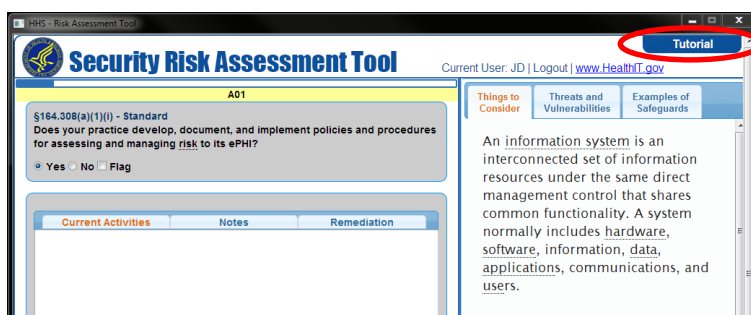


Figure 43

When you log back in, all previous answers are saved. For more information on how to use the tool, select the “Tutorial” button located on the upper right.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

**Figure 44**

As previously stated, the SRA Tool will save the answers based on the internet protocol (IP) address used by the computer or server.

2.5 Clearing stored data on the SRA Tool (Windows 7 version)

To clear all data within the SRA Tool, open your windows start menu by selecting the “Start” button located on the bottom left.

**Figure 45**

Next, locate the search bar at the very bottom left. Insert the following text exactly as it appears (without the quotations; case sensitive), “%LOCALAPPDATA%” and hit enter.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

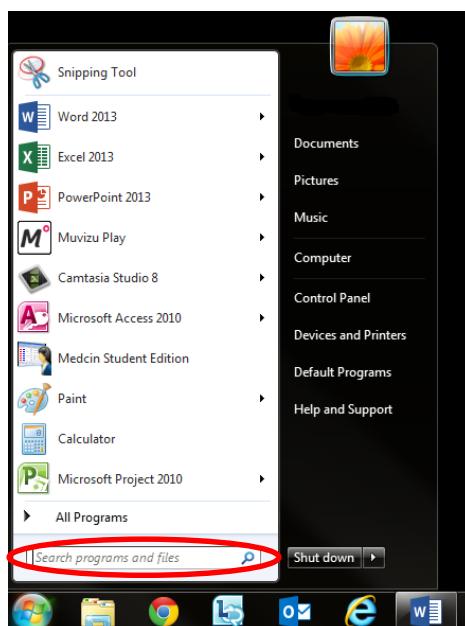


Figure 46

Once you press the enter key on your keyboard, a pop-up window will display. Locate the folder titled, “HHS” and delete it. After deleting this folder, all information within the SRA Tool will be cleared. Once you delete the “HHS” folder, you will not be able to retrieve previous data from the SRA Tool unless you restore folder.

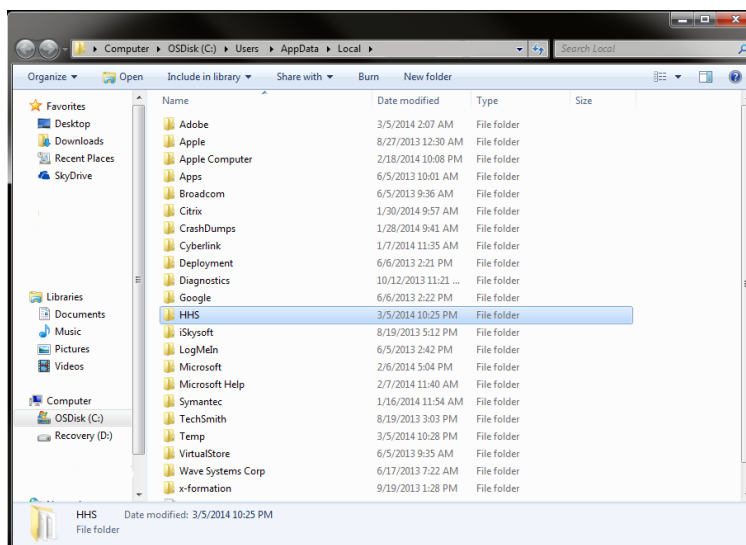


Figure 47

To restore the folder, simply navigate to your trash folder located within your desktop or laptop, select the “HHS” folder and click on “Restore this item.” Your “HHS” folder will automatically be restored to its original location and you will be able to see the previous data.

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule’s requirements for risk assessment and risk management.

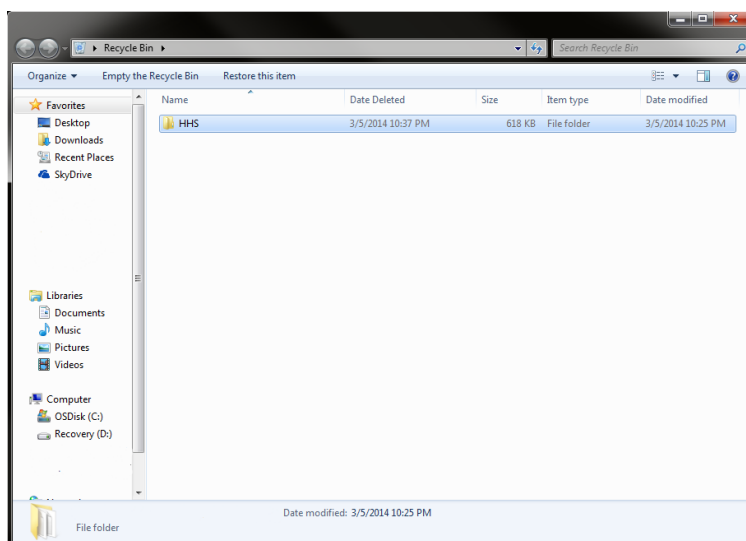


Figure 48

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management.



3.0 Appendix A

REQUIRED AND ADDRESSABLE SPECIFICATIONS:

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

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

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. For example, 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. For more information: <http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2020.html>

*The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management.