



National Institute of Standards and Technology

HIPAA Security Rule Toolkit User Guide

October 31, 2011

Table of Contents

Background.....	1
Purpose.....	1
Audience	1
Intended Use of the HSR Toolkit.....	1
What the HSR Toolkit Is	2
The Role of the HSR Toolkit in a Risk Assessment.....	2
What the HSR Toolkit Is Not	3
How to Approach Questions.....	4
Case Study #1	4
Case Study #2	5
Main Menu.....	6
File Tab Functions	7
Reports Tab Functions	7
Tools Tab Functions	8
Help Tab Functions.....	8
Getting Started.....	9
Set up a Profile.....	9
Open a New Survey.....	11
Continue a Survey	12
Questionnaire Navigation	13
Select a Topic Area	14
Answer Survey Questions	14
Generate a Report.....	16
What Highlighting Means.....	17
Flags and Icons	18
Appendix A – Acronyms.....	19

List of Figures

Figure 1. HSR Toolkit Main Screen	6
Figure 2. Profile Manager Screen	9
Figure 3. Profile Manager Screen	11
Figure 4. The Start Questionnaire Screen	12
Figure 5. The Survey Dashboard Screen	13
Figure 6. The Questionnaire Screen.....	14
Figure 7. Attachments Box.....	15
Figure 8. Reports Menu	16
Figure 9. Report Save Dialogue.....	16
Figure 10. Example of Highlighting	17
Figure 11. Example of Icons	18
Figure 12. Example of the Flagging Function	18

National Institute of Standards and Technology (NIST)**HIPAA Security Rule Toolkit****User Guide****Background**

NIST has been involved in Health Information Technology (HIT) research since 1994 and, through the American Recovery and Reinvestment Act (ARRA) of 2009, is playing a major role in accelerating the development and harmonization of standards and developing conformance test tools for HIT.

The Health Insurance Portability Accountability Act (HIPAA) Security Rule (45 CFR 160, 162, and 164) establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The HIPAA Security Rule Toolkit (HSR Toolkit) application targets users who include, but are not limited to, HIPAA-covered entities and business associates, and other organizations, such as those providing HIPAA Security Rule implementation, assessment, and compliance services. Target user organizations can range in size from a large nationwide health plan with vast information technology (IT) resources to a small health care provider with limited access to IT expertise.

Purpose

The purpose of the NIST HSR Toolkit project is to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environments.

Audience

The HSR Toolkit is intended to be used by any organization, including covered entities and business associates that wish to augment their understanding and implementation of the HIPAA Security Rule. This spans the entire spectrum of healthcare entities from very large organizations with vast IT resources to very small businesses and provider practices that may have limited access to IT expertise.

Intended Use of the HSR Toolkit

The HSR Toolkit is intended to be one of many useful resources that users can leverage. Although the Toolkit application has been developed by NIST, NIST is not a regulatory or enforcement authority for the HIPAA Security Rule. The HSR Toolkit is ***not*** intended to make any statement of an organization's compliance with the requirements of the HIPAA Security Rule. Statements of compliance are the responsibility of the covered entity and the regulatory

and enforcement authority, which, in the case of the HIPAA Security Rule, is the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

Large organizations can use the HSR Toolkit to supplement their risk assessment processes conducted by their security offices. The Toolkit may also be used to assist in alignment across multiple operating units. Small organizations can utilize the Toolkit to gain a better understanding of the current status of their HSR implementation, and to serve as input into an action plan for implementation improvements.

What the HSR Toolkit Is

The HSR Toolkit is a desktop-based application that is intended to be a useful resource among a set of tools and processes that an organization can use to assist in reviewing its implementation of the HSR. It is a self-contained, operating system (OS) independent application that can be run on various environments, including Windows, Red Hat Linux, and Apple OS X platforms. The security content that makes up the question set will provide support that other organizations can reuse over and over again.

The HSR Toolkit addresses the 45 implementation specifications identified in the HIPAA Security Rule and cover basic security practices, security failures, risk management, and personnel issues. Basic security practice questions include defining and managing access, backups, recoveries, and physical security. Questions addressing security failures deal with legal items to attend to after an incident, such as breach notifications. 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.

The sources of information used to support the development of the HSR Toolkit questionnaires include the following:

- HIPAA Security Rule
- 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

The Role of the HSR Toolkit in a Risk Assessment

Use of the HSR Toolkit 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 HSR Toolkit 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.

What the HSR Toolkit Is Not

A Multi-User Tool. The HSR Toolkit 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 with appropriate permissions to install and run the application on the desktop will use the tool to individually capture information. Both complete and in-process data gathered during a survey will be saved in a separate and distinct data file (XML) that itself can be shared. Another user may individually **import** that saved file and continue the survey.

A Compliance Tool. The HSR Toolkit does not produce a statement of compliance. Organizations may use the HSR Toolkit in coordination with other tools and processes to support HIPAA Security Rule compliance and risk management activities. Statements of compliance are the responsibility of the covered entity and the HIPAA Security Rule regulatory and enforcement authority.

A HIPAA Privacy Rule Tool. The HSR Toolkit provides guidance in understanding the requirements of the HIPAA Security Rule specifically, and does not include provisions for the HIPAA Privacy Rule.

How to Approach Questions

Most of the questions in the Toolkit can be answered by one of three choices:

- **Yes**
- **No**
- **Not Applicable**

Selecting either **Yes** or **No** is neither inherently correct nor incorrect. The answer truly depends upon the size, implementation, and manner of justification provided by the respondent. Why is this important? Consider the case studies below.

Case Study #1

In the following example, the question involves a number of elements to be addressed in an organizations' risk assessment policy.

Case Study #1 Question: *Does your organization's risk assessment policy address: purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, training, and compliance?*

Instructions:

*--If yes, select **Yes** below.*

*--If no, select **No** below.*

It may be that an organization has addressed some but not all of these elements in its risk assessment policy documentation. If *training* and *compliance* were not addressed in the documentation, should the user select the **No** option?

Not necessarily.

This will be a subjective evaluation after the pertinent documentation has been examined. The user may feel that all elements of the question have been addressed and therefore feels justified in selecting the **Yes** option. This can be true for any size organization. In either case, it is suggested that the user make liberal use of the comments box. In this case, it is valid to choose either **Yes** or **No**.

Case Study #2

In the following example, the user is asked to supply an answer and supporting information to justify that answer.

Case Study #2 Question: *When your organization audits your information system, does the audit information reside in a separate server?*

Instructions:

*--If yes, select **Yes** below and please name where.*

*--If no, select **No** below and please explain.*

In both situations, the user is requested to document supplemental information in the comment field. In many instances, the user is encouraged to make extensive use of the comment field to provide additional information, reference internal documents, or add simple notes on a topic to refer to later. Depending upon the manner in which an organization wishes to use the Toolkit, the comments field can hold internal notes and detailed descriptions as to why a requirement was or was not addressed.

Main Menu

The *Main Menu* is a series of four tab options from which you can manage surveys, generate reports, review specific settings about the operation of the Toolkit, and gather additional information regarding the Toolkit. A survey is a complete set of HSR questions and recorded answers organized by safeguard family.

The *Main Menu* screen is shown in **Figure 1**.

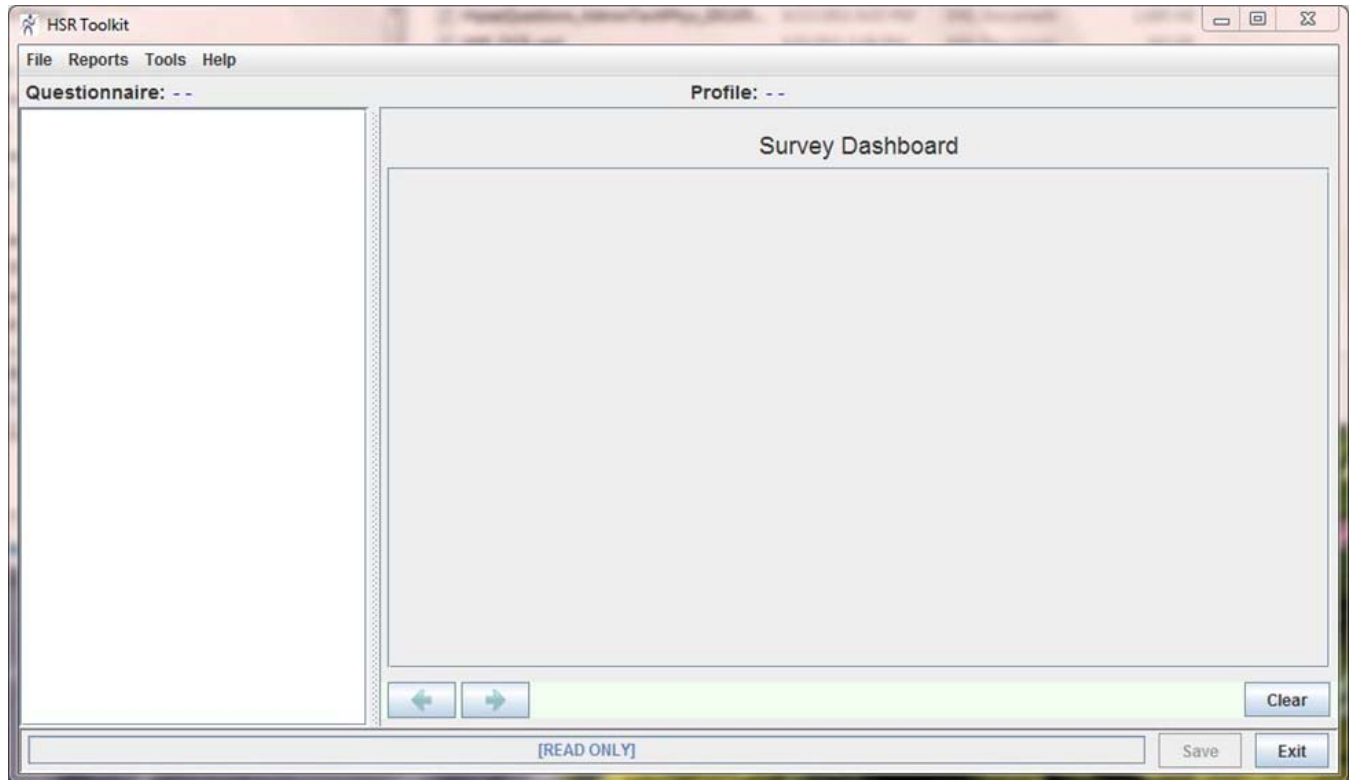


Figure 1. HSR Toolkit Main Screen

Descriptions of each of the Main Menu tabs follow.

File Tab Functions

Function	Description
New	Presents a submenu to select a survey type.
New ► Enterprise Survey	Loads a new survey questionnaire from the complete set of HSR questions. <i>This is suggested for large and mid-sized organizations.</i>
New ► Standard Survey	Loads a new survey questionnaire from the abridged set of HSR questions. <i>This is suggested for small organizations.</i>
Resume	Opens an existing survey for editing.
Import	Enables the import of XML files to populate a survey.
Save	Saves your work to a file that you name.
Save As	Saves your work to a new file that you name.
Exit	Exits the HSR Toolkit application.

Reports Tab Functions

Function	Description
HSR Safeguard Families	Generates a summary report of the number of questions within each safeguard family and the number of questions that were answered.
Flagged Items ► Order By Flag Level	Generates a detailed report of only flagged questions and the associated answers ordered by flag level. For example, all questions and answers at level 1, then all questions and answers at level 2, etc.
Flagged Items ► Order By Appearance	Generates a detailed report of only flagged questions and the associated answers ordered by safeguard family. For example, all flagged questions in administrative safeguards, then technical safeguards, etc.
Uncommented Questions	Generates a detailed report of only questions that do not have any comments associated with them.
All	Generates a complete and detailed report of all questions and answers.

Tools Tab Functions

Function	Description
Profile Manager	Enables you to create a new profile, clear or delete an existing profile, and save profile information.
Show Dashboard	Displays the Survey Dashboard in the main reading pane.
Personnel Settings	Enables you to customize your settings regarding: <ul style="list-style-type: none"> • Updates to the HIPAA Security Rule • Preference for file folder location of saved surveys • Upon accessing a new survey, a prompt asking if you would like to use the default template survey

Help Tab Functions

Function	Description
User Guide	Presents a copy of the HSR Toolkit User Guide.
Check for Updates	Generates a check for updates to the HIPAA Security Rule content and application.
About	Provides the version number and date of this HSR Toolkit application, and additional information regarding the software used in creating this application.

Getting Started

Set up a Profile

1. On the **Tools** tab, select **Profile Manager**. The *Profile Manager* window will appear, as shown in **Figure 2**.

Figure 2. Profile Manager Screen

2. Select the **New** button. The *Edit Profile Identifier* box will appear.
3. Fill in your type of entity (provider, hospital, etc.) or another identifier specific to the subject being assessed and select **OK**.
4. Fill in the rest of the profile information on the assessment subject and the assessor.

Field	Profile Information
Assessment Subject	
Subject	Name of the assessment subject (for example, the organization name)
Type	Type of assessment subject (for example, covered entity, business associate)
Scope	Scope of assessment subject (for example, entire organization, one unit, or one system)
Description	Any brief introduction/comments about this subject

Field	Profile Information
Assessor	
First Name	Assessor's first name
Last Name	Assessor's last name
Phone	Assessor's phone number
Location	Assessor's location
E-Mail	Assessor's email address

5. Select **Save** to preserve the information.
6. Select **Close** to return to the main screen.

Open a New Survey

1. On the **File** tab, select **New** to populate a new survey. The *Profile Manager* screen will appear, as shown in **Figure 3**.

The screenshot shows a window titled "Profile Manager" with a close button in the top right corner. The window is divided into two main sections: "Assessment Subject" and "Assessor".

Assessment Subject Section:

- Profile:** A dropdown menu showing "Davis Memorial Medical Center" with a "Change Name" button to its right.
- Subject:** A text field containing "The Davis Memorial Medical Center".
- Type:** A dropdown menu showing "Hospital".
- Scope:** A dropdown menu showing "Entire Hospital Records".
- Description:** A text area containing "An evaluation of all medical records and data recorded for patients of the medical center will be evaluated."

Assessor Section:

- First Name:** A text field containing "Mary".
- Last Name:** A text field containing "Smith".
- Location:** A text field containing "1413 Medical Center Drive, Anytown, MD 25555".
- Phone:** A text field containing "301-555-1245".
- E-Mail:** A text field containing "msmith@DMMC.org".

Buttons: At the bottom of the window, there are six buttons: "Save", "Save As...", "Clear", "Delete", "Use Selected", and "Close".

Figure 3. Profile Manager Screen

2. From the **Profile** drop-down menu, select the profile to be evaluated. Alternatively, if the desired profile does not populate automatically, click on the **Change Name** button, select a new profile, and click on **OK**.
3. Click on **Close** to complete this step and return to the main screen.
4. The **Clear** button clears the form elements for the active profile.
5. The **Delete** button will delete the actively selected profile.

Continue a Survey

1. On the **File** tab, select **Resume**. The *Start Questionnaire* screen will appear, as shown in **Figure 4**.

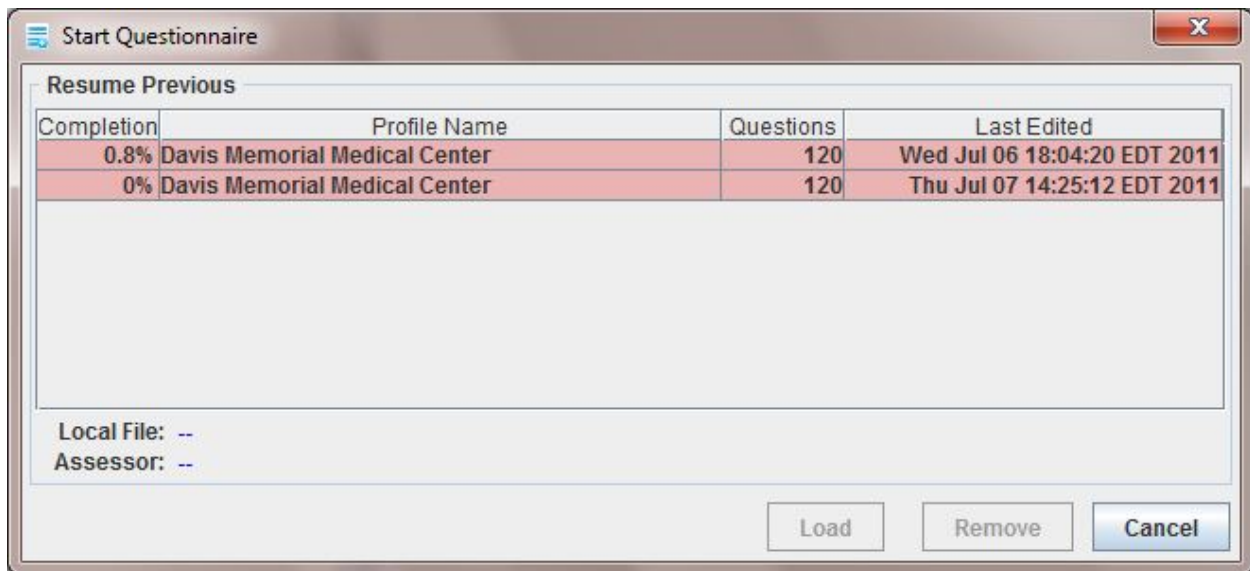


Figure 4. The Start Questionnaire Screen

2. Select the survey you wish to work on and click on **Load**. The selected survey will populate in the Toolkit and the *Survey Dashboard* window will appear.

Questionnaire Navigation

Whether you selected the Standard Survey or the Enterprise Survey, the Survey Dashboard will appear as shown in **Figure 5**. The Enterprise Survey, however, will contain many more questions than the Standard Survey.

The Questionnaire navigation pane shown in **Figure 5** allows you to quickly navigate the questions in the HIPAA Security Rule Checklist. It shows the relationship of questions to their policy specification and safeguard family. The navigation appears in a tree menu, so that by clicking on a parent or folder-level item, it expands to show the subordinate categories or questions. Questions themselves appear in the main window pane to the right and allow you to record your answers. The navigation also shows which questions have been answered (shown by a checkmark) and which have not (shown by a blank or red radio button).

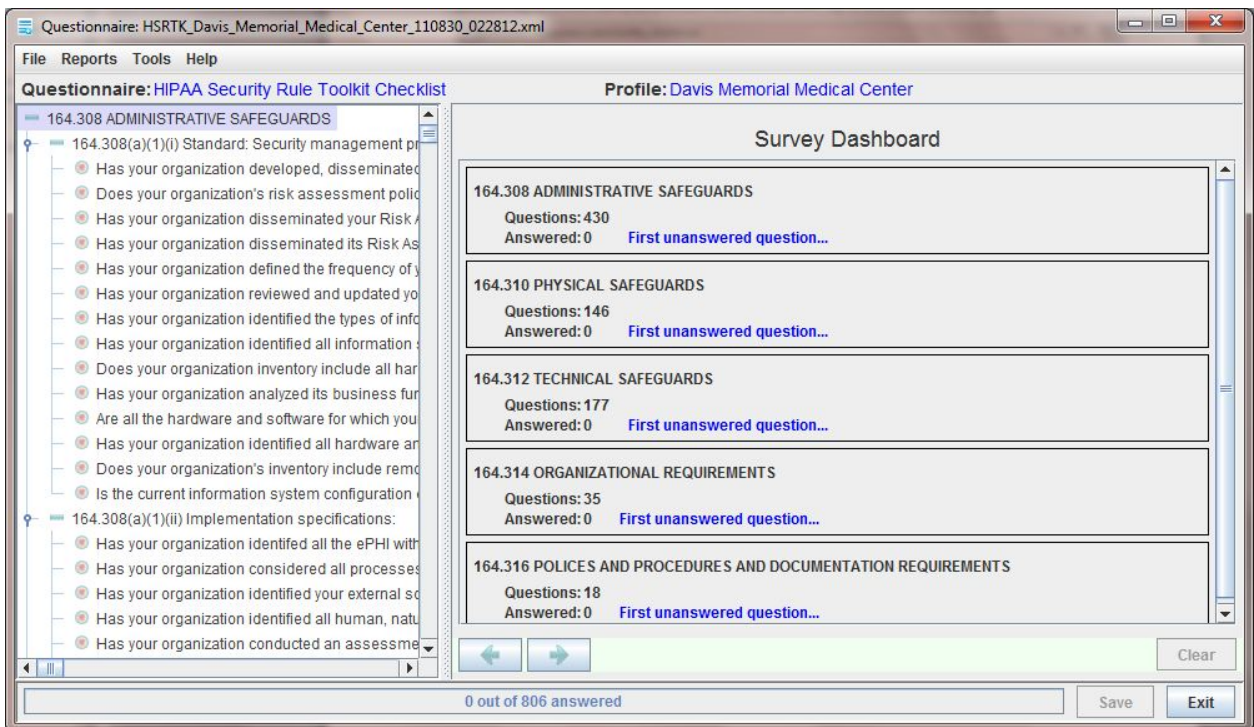


Figure 5. The Survey Dashboard Screen

Select a Topic Area

1. The *Survey Dashboard* shows five topic areas:
 - Administrative Safeguards
 - Physical Safeguards
 - Technical Safeguards
 - Organizational Safeguards
 - Policies and Procedures and Documentation Requirements

The survey will also automatically populate with HIPAA Security Rule questions pertaining to each of the five safeguard areas, as shown in **Figure 6**.

Figure 6. The Questionnaire Screen

Answer Survey Questions

1. On the left-hand pane of the survey, choose a question to answer by highlighting and selecting it. The selected question will appear in the *Question Text* box, as shown in **Figure 6**.
2. Click on the appropriate radio button (**Yes**, **No**, or **Not Applicable**) to answer the question.
3. Type any applicable comments in the *Comments* box.

4. Attach any applicable documents by selecting the **Add** button in the *Attachments* window. A window of your available files will appear. Highlight the appropriate files (Word, Excel, and pdf file formats are all acceptable) and select **Open**. The attached file will appear in the *Attachments* box shown in **Figure 7**.

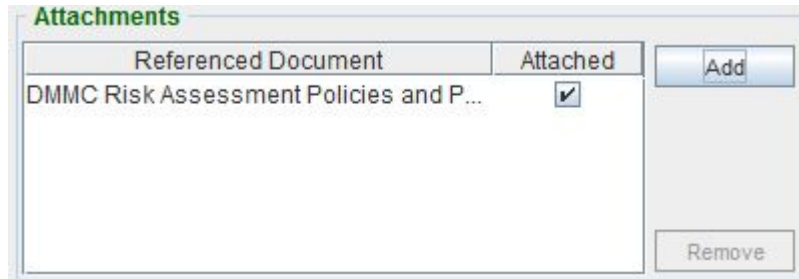



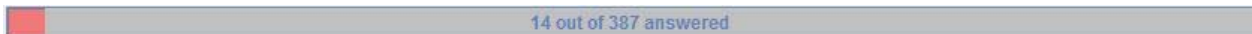


Figure 7. Attachments Box

5. Choose the question you wish to answer next by highlighting and selecting it or by using the arrow keys at the bottom of the Survey Dashboard to move to the next or previous question. 
6. A blank radio button in front of a question indicates the question has not yet been answered. 
7. A checkmark in front of a question indicates the question has been answered. 
8. A status bar at the bottom of the Survey Dashboard provides both a numerical and a color-coded status of how many questions have been answered.



9. Select **Save** to preserve your information.

Quick Tip: You do not have to **Save** after each question. The information you input will remain in the memory.

You can save your work at any time, however, and you will be prompted to save your work before you exit the survey.

Generate a Report

1. On the **File** tab, select **Reports**. A submenu will appear that identifies the types of reports available for creation, as shown in **Figure 8**.

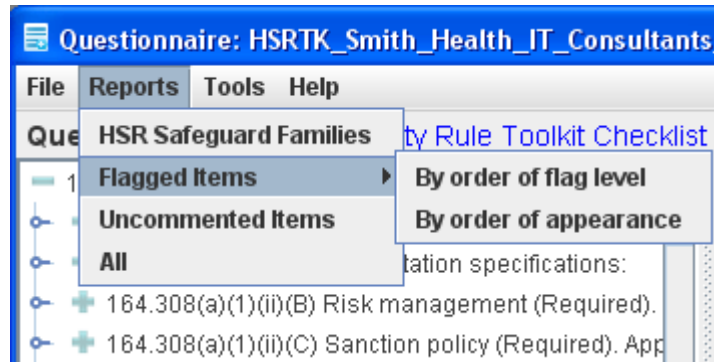


Figure 8. Reports Menu

2. Once a report type is selected, a dialogue box, as demonstrated in **Figure 9**, will prompt you to **Save** the selected report in the default reports directory.

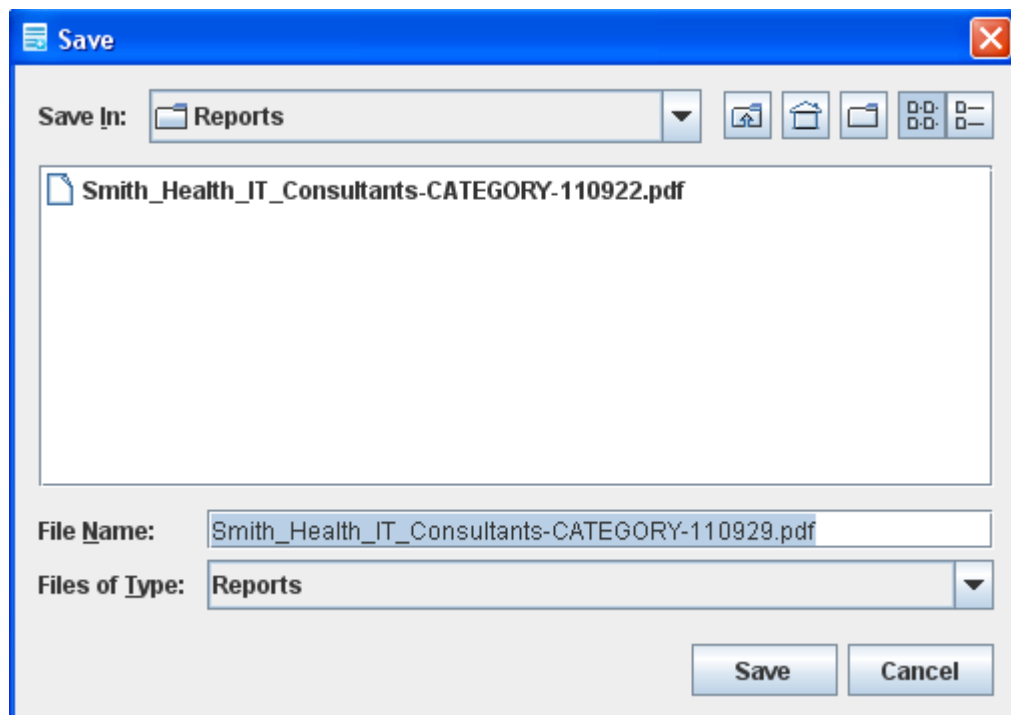


Figure 9. Report Save Dialogue

3. Once a report type is selected, a dialogue box, like the one shown in **Figure 9**, will prompt you to **Save** the selected report in the default reports directory. You have the option to click **Save** to create the report or **Cancel** to cancel the operation.
4. If **Save** is selected, a window will pop up that displays the final report.

What Highlighting Means

In many places where a question references either an explanation or an attachment to be selected, the comment field and/or the attachment field will be highlighted, as shown in **Figure 10**, indicating that supporting information is requested in this field.

The screenshot shows the 'Questionnaire: HIPAA Security Rule Toolkit Checklist' application. The left pane lists various questions under '164.308 ADMINISTRATIVE SAFEGUARDS'. The main pane displays a specific question: 'Has your organization developed, disseminated, reviewed/updated, and trained on your Risk Assessment policies and procedures?'. Below the question text are instructions and a 'References' section. The 'Attachments' and 'Comments' fields are highlighted in green. The 'Attachments' field has a table with columns 'Referenced Document' and 'Attached', and buttons 'Add' and 'Remove'. The 'Comments' field is a text area. At the bottom, there are navigation buttons and a status bar indicating '1 out of 14 answered'.

Figure 10. Example of Highlighting

Should the highlighting appear, it does not mean that supporting information is required. Since the application does not evaluate compliance, providing information is optional but may be beneficial to the organization conducting the assessment. Additionally, the user is free to use both the Attachments and Comments field, and the use of either will not affect the function or evaluation of the Toolkit.

Flags and Icons

When reviewing questions, the user may find that an attachment or a comment is requested to support the selected answer. Where the supporting attachment or comment is not provided, the Toolkit application displays a yellow triangular warning icon in the menu navigation, as shown in **Figure 11**.

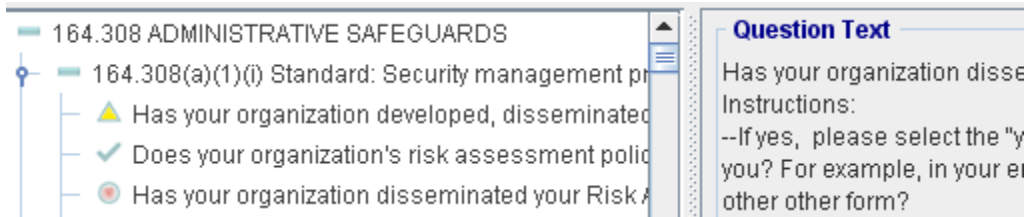





Figure 11. Example of Icons

Icon	Description
	A yellow warning icon indicates that a supporting attachment or comment was not provided.
	A green checkmark indicates that the question has been answered and the requested supplemental information has been addressed.
	A red target icon indicates that the question has not been answered.

Additionally, the Toolkit provides a flagging function, shown in **Figure 12**, where the user can assign a level of priority to a question. A choice of levels 1 through 5 can be assigned to a question. That level is then reflected by an additional icon of the same value in the menu navigation.

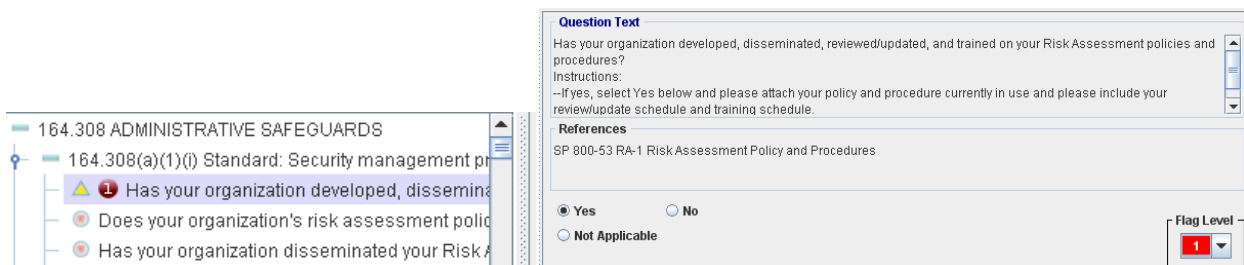


Figure 12. Example of the Flagging Function

The flag level does not indicate severity or evaluation. It is suggested that the performing organization use this to manage the questions and the response content according to its internal processes. It is the responsibility of the performing organization to define the use and values of the flag levels.

Appendix A – Acronyms

ARRA	American Recovery and Reinvestment Act
EPHI	Electronic Protected Health Information
HIPAA	Health Insurance Portability Accountability Act
HIT	Health Information Technology
HITECH	Health Information Technology for Economic and Clinical Health Act
HHS	Department of Health and Human Services
HSR	HIPAA Security Rule
OCIL	Open Checklist Interactive Language
OCR	Office of Civil Rights (HHS)