NETWORK DETECTIVE™

QUICK START GUIDE

HIPAA Compliance Assessment Module

Instructions to Perform a HIPAA Compliance Assessment

11/2/2023 4:51 PM

Contents

Performing a HIPAA Compliance Assessment

HIPAA Compliance Assessment Overview

Network Detective’s HIPAA Compliance Assessment Module combines 1) automated data collection with 2) a structured framework for collecting supplemental assessment information through surveys and worksheets. To perform a HIPAA Compliance Assessment, you will:

- Download and install the required tools
- Create a site and set up a HIPAA Compliance Assessment project
- Collect HIPAA Compliance Assessment data using the Network Detective Checklist
- Generate HIPAA Compliance Assessment reports

What You Will Need

In order to perform a HIPAA Compliance Assessment, you will need the following components:

Note: You can access these at https://www.rapidfiretools.com/nd.

HIPAA Compliance Assessment Component	Description
Network Detective	The Network Detective Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
HIPAA Data Collector	The Network Detective HIPAA Data Collector is a windows application that performs the data collections for the HIPAA Compliance Module. Supports both the Network and Computer scans.
Push Deploy Tool	The Network Detective Push-Deploy Tool pushes the local data collector to machines in a specified range and saves the scan files to a specified directory (which can also be a network share). The benefit of the tool is that a local scan can be run simultaneously on each computer from a centralized location.
Surveys and Worksheets	Surveys and worksheets contain questions that require investigation outside of an automated scan. You create and manage these documents directly from the Network Detective Application, where you can also import and export your responses to and from Word.

Risk Assessment vs. Risk Profile

There are two types of HIPAA Compliance Assessments that can be performed:

Assessment Type	Description
HIPAA Risk Assessment	A complete assessment that includes all worksheets and surveys. • Required at least annually • Recommended quarterly as part of a quarterly compliance review • Requires that all manual worksheets be completed **Important:** Allow for at least an entire day to perform the assessment on a typical 15 user network
HIPAA Risk Profile	Updates a Risk Assessment to show progress in avoiding and mitigating risks - and finds new ones that may have otherwise been missed. • Does NOT require worksheets • Requires selecting a prior Risk Assessment (will use existing worksheets) • Requires less than 1 hour for a typical 15 user network **Note:** You can only create a Risk Profile after you have first performed a Risk Assessment.

HIPAA Risk Profile Use for Ongoing HIPAA Compliance Assessments

A HIPAA Risk Analysis should be done no less than once a year. However, the Network Detective includes an abbreviated version of the HIPAA Risk Analysis assessment and reporting process within the Network Detective HIPAA Module. This process is called the HIPAA Risk Profile.

The HIPAA Risk Profile is designed to provide interim reporting in a streamlined and almost completely automated manner.

Whether performed monthly or quarterly, the Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks, and finds new ones that may have otherwise been missed and resulted in a data breach.

An important aspect of this abbreviated process is the need that the HIPAA Module has been already used to perform a HIPAA Risk Assessment of your customer’s network on a previous occasion.

Using the Security Exception Worksheet to Address Compliance Lapses and False Positives

Sometimes you may get stuck in an assessment. This might happen for several reasons:

- You cannot resolve every single compliance issue identified in the assessment
- Your scan results differ from what you know is the reality on the target network
- You do not have enough information to enter accurate responses for every form question

If you encounter any of the above, you can always move ahead and complete your assessment using the **Security Exception Worksheet**. This worksheet becomes available near the end of your To Do list. It allows you to document explanations on suspect items. Your explanation can include why various discovered items are not true issues and indicate possible false positives. Additionally, you can explain why a certain compliance requirement should not apply to you – or an alternative way in which you have met the requirement.

These exceptions can be documented on an item by item level (for example: at the granularity at users, ports, applications, etc.). The **Security Exception Worksheet** does not alleviate the need for safeguards but allows for description of alternative means of mitigating the identified security risk.

Follow these steps to perform a HIPAA Compliance Assessment:

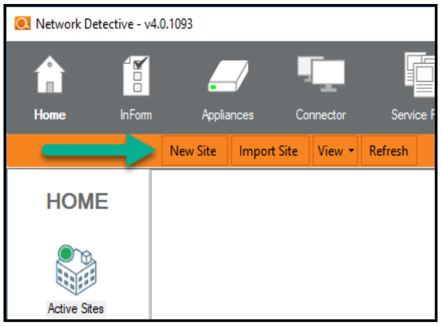
Step 1 — Download and Install the Network Detective Application

Visit https://www.rapidfiretools.com/nd. Download and install the Network Detective Application.

Step 2 — Create a New Site

To create a new site:

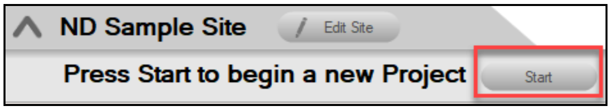
1. Open the Network Detective Application and log in with your credentials.
2. Click **New Site** to create a new Site for your assessment project.



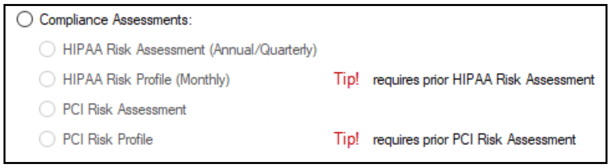
3. Enter a **Site Name** and click **OK**.

Step 3 — Start a HIPAA Compliance Assessment Project

1. From within the Site Window, click **Start** to begin the assessment.



2. Next, select **Compliance Assessments**, and then select your chosen HIPAA Compliance Assessment.



○ Compliance Assessments:

○ HIPAA Risk Assessment (Annual/Quarterly)

○ HIPAA Risk Profile (Monthly) Tip! requires prior HIPAA Risk Assessment

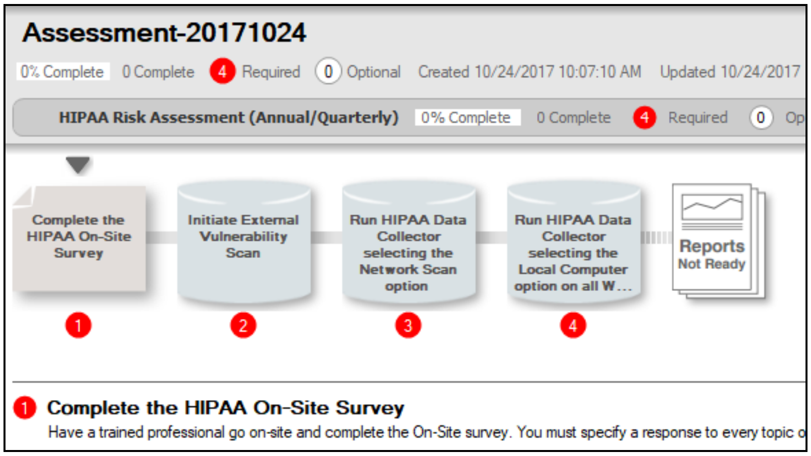
○ PCI Risk Assessment

○ PCI Risk Profile Tip! requires prior PCI Risk Assessment

3. Then follow the prompts presented in the Network Detective Wizard to start the new Assessment.

Use the HIPAA Compliance Assessment Checklist

Once you begin the HIPAA Compliance Assessment, a **Checklist** appears in the Assessment Window. The **Checklist** presents the **Required** 1 and **Optional** 1 steps that are to be performed during the assessment process. The **Checklist** will be updated with additional steps to be performed throughout the assessment process.



Assessment-20171024

0% Complete 0 Complete 4 Required 0 Optional Created 10/24/2017 10:07:10 AM Updated 10/24/2017

HIPAA Risk Assessment (Annual/Quarterly) 0% Complete 0 Complete 4 Required 0 Op

1 Complete the HIPAA On-Site Survey

2 Initiate External Vulnerability Scan

3 Run HIPAA Data Collector selecting the Network Scan option

4 Run HIPAA Data Collector selecting the Local Computer option on all W…

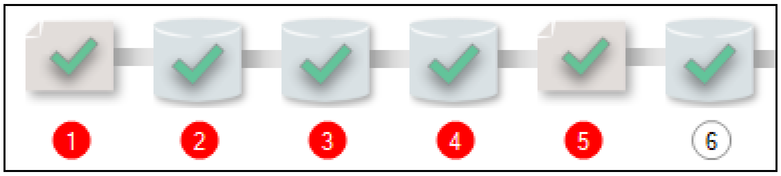
Reports Not Ready

1 **Complete the HIPAA On-Site Survey**

Have a trained professional go on-site and complete the On-Site survey. You must specify a response to every topic o

Complete the required **Checklist Items** in the exact numerical order presented. Use the **Refresh Checklist** feature to guide you through the assessment process at each step until completion.

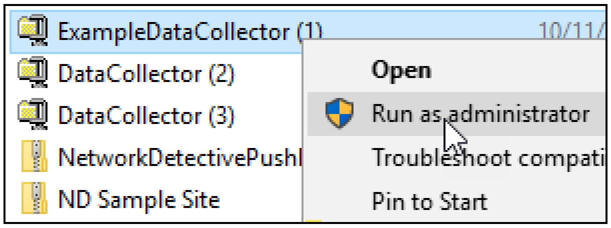
When you complete a step, that item will be updated with a green check mark ✓ in the checklist.



You may also print a copy of the **Checklist** for reference purposes by using the **Printed Checklist** feature.

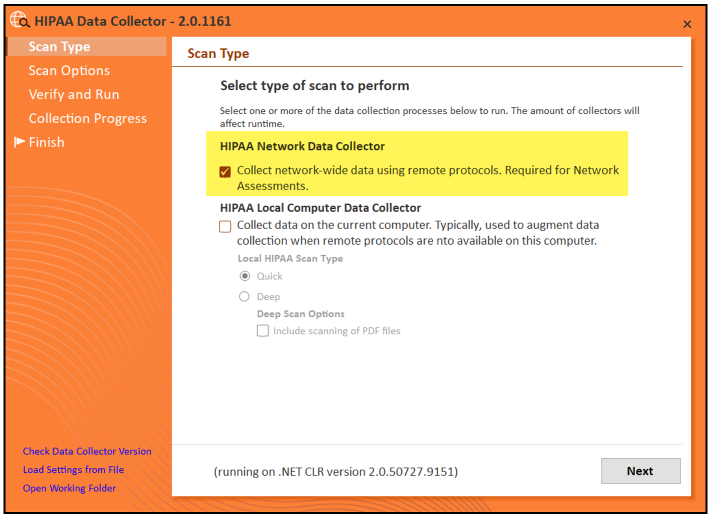
Step 4 — Collect Initial HIPAA Compliance Assessment Data

1. Complete the **HIPAA On-site Survey**. View the assessment **Checklist** for updates and to track progress.
2. Initiate the **External Vulnerability Scan**.
3. Download and run the **HIPAA Data Collector** from www.rapidfiretools/nd. Be sure to run the **Data Collector** as an **Administrator**.



Important: For the most comprehensive scan, you MUST run the data collector as an ADMINISTRATOR.

4. Select the **HIPAA Network Data Collector** and complete all required prompts to initiate the scan.



Scan Type

Select type of scan to perform

Select one or more of the data collection processes below to run. The amount of collectors will affect runtime.

HIPAA Network Data Collector

☑ Collect network-wide data using remote protocols. Required for Network Assessments.

HIPAA Local Computer Data Collector

☐ Collect data on the current computer. Typically, used to augment data collection when remote protocols are nto available on this computer.

Local HIPAA Scan Type

● Quick

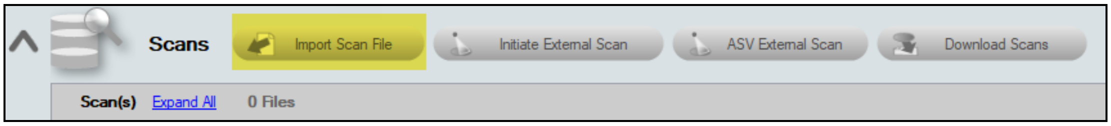
○ Deep

Deep Scan Options

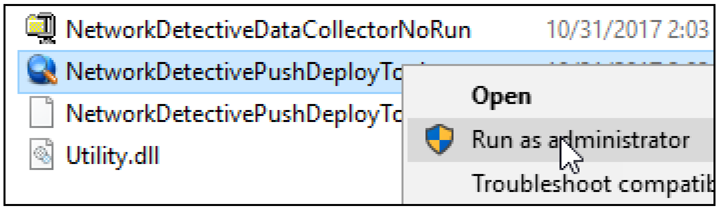
☐ Include scanning of PDF files

(running on .NET CLR version 2.0.50727.9151)

5. **Import** the scan results into your assessment.

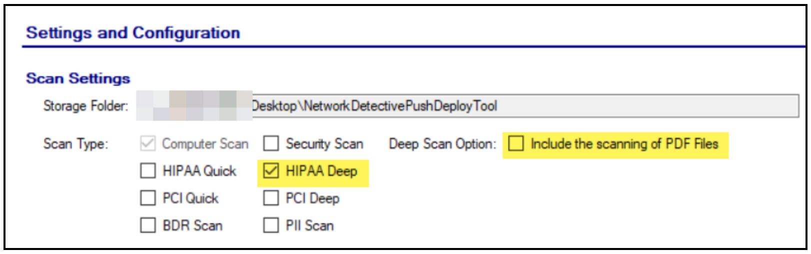


6. Next, to perform the **HIPAA Local Computer Scans** of computers on the network, download and install the Push Deploy Tool on your USB drive from https://www.rapidfiretools.com/nd.
7. Then extract the contents of the **Network Detective Push Deploy Tool .ZIP** file to a USB drive or directly to any machine on the target network.
8. Using the **Run as Administrator** option, run the **NetworkDetectivePushDeployTool.exe** contained within the folder named **NetworkDetectivePushDeployTool**.


NetworkDetectiveDataCollectorNoRun
10/31/2017 2:03
NetworkDetectivePushDeployTo
NetworkDetectivePushDeployTo
Utility.dll
Open
Run as administrator
Troubleshoot compatib

Important: For the most comprehensive scan, you MUST run the Push Deploy Tool as an ADMINISTRATOR.

9. From the tool's Settings and Configuration window, select the **HIPAA Deep Scan** option.



Settings and Configuration

Scan Settings

Storage Folder: [redacted]Desktop\NetworkDetectivePushDeployTool

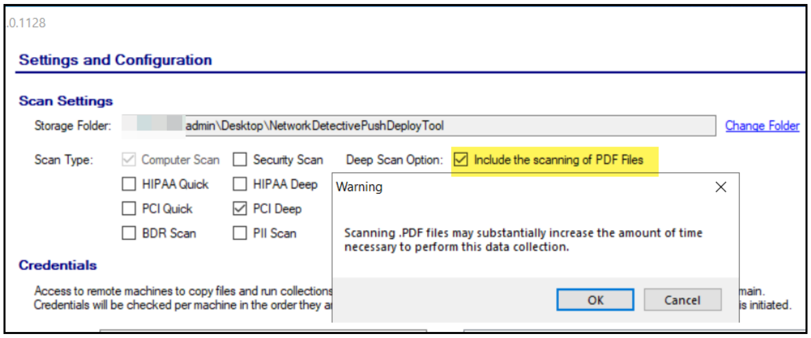
Scan Type: ☑ Computer Scan ☐ Security Scan Deep Scan Option: ☐ Include the scanning of PDF Files

☐ HIPAA Quick ☑ HIPAA Deep

☐ PCI Quick ☐ PCI Deep

☐ BDR Scan ☐ PII Scan

Also select whether you want to scan PDF files. Note that this may significantly increase total scan time.



.0.1128

Settings and Configuration

Scan Settings

Storage Folder: [redacted]admin\Desktop\NetworkDetectivePushDeployTool Change Folder

Scan Type: ☑ Computer Scan ☐ Security Scan Deep Scan Option: ☑ Include the scanning of PDF Files

☐ HIPAA Quick ☐ HIPAA Deep

☐ PCI Quick ☑ PCI Deep

☐ BDR Scan ☐ PII Scan

Credentials

Access to remote machines to copy files and run collections main.
Credentials will be checked per machine in the order they a is initiated.

Warning ×

Scanning .PDF files may substantially increase the amount of time necessary to perform this data collection.

OK Cancel

10. Specify the **Folder** to store resulting computer scan files, and enter any additional **Administrator Credentials** that are necessary. Then, click the **Next** button.

Important: For the **Push Deploy Tool** to push local scans to computers throughout the network, ensure that the following prerequisites are met:

• **Ensure that the Windows Management Instrumentation (WMI) service is running** and able to be managed remotely on the computers that you wish to scan. Sometimes Windows Firewall blocks Remote Management of WMI, so this service may need to be allowed to operate through the Firewall.

• **Admin$ must be present on the computers you wish to scan**, and be accessible with the login credentials you provide for the scan. Push/Deploy relies on using the Admin$ share to copy and run the data collector locally.

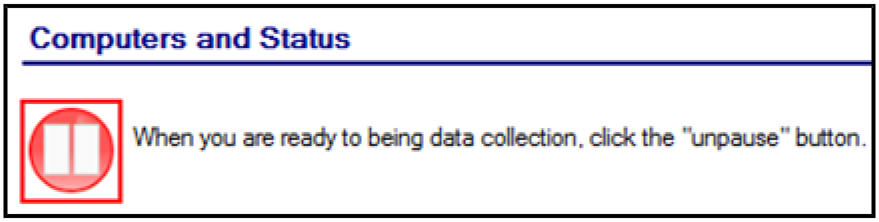
• **File and printer sharing must be enabled** on the computers you wish to scan.

• **For Workgroup based networks, the Administrator credentials for all workstations and servers that are to be scanned are recommended to be the same**. In cases where a Workgroup-based network does not have a one set of Administrator credentials for all machines to be scanned, use the Add option to add all of the Administrator credentials for the Workgroup. Multiple sets of Administrator credentials will be listed in the Credentials box.

Tip: For your convenience, create a shared network folder to centralize and store all scan results data files created by the **Push Deploy Tool**. Then reference this folder in the **Storage Folder** field to enable the local computer scan data files to be stored in this central location.

11. In the **Computers and Status** window presented, set the **IP Address range** of the computers to be scanned and then run the scan. After defining the computer **IP Address range**, click the “**unpause**” button as instructed to start your data collection scan.

    Alternatively, you can click the **Next** button where you will be prompted to start the data collection process.



Computers and Status

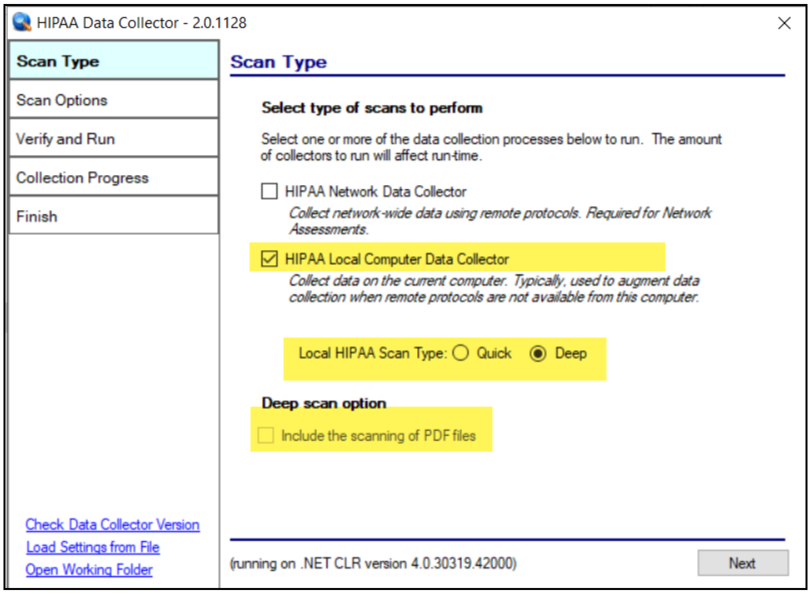
When you are ready to being data collection, click the "unpause" button.

After starting the data collection, the **Computers and Status** window will present the status of the scan for each computer selected for scanning.

12. When the data collection process is complete, click **Next** to proceed to the **Collected Data Files** window within the **Push Deploy Tool**. Click the **Finish** button to complete the **Push Deploy Tool** data collection process and to access the scan files produced.
13. Next **Import** the scan results contained in the .ZIP file(s) produced by the **Push Deploy Tool** into your assessment.

Step 5 — Collect Secondary Data

1. Run the **HIPAA Local Computer Data Collector** selecting the **Deep Scan** to be performed on the computers that were unreachable during the Local Scans run using the **Push Deploy Tool**. Also specify whether to include PDF files in the scan.



Scan Type

Select type of scans to perform

Select one or more of the data collection processes below to run. The amount of collectors to run will affect run-time.

☐ HIPAA Network Data Collector
Collect network-wide data using remote protocols. Required for Network Assessments.

☑ HIPAA Local Computer Data Collector
Collect data on the current computer. Typically, used to augment data collection when remote protocols are not available from this computer.

Local HIPAA Scan Type: ○ Quick ● Deep

Deep scan option

☐ Include the scanning of PDF files

(running on .NET CLR version 4.0.30319.42000)

> **Note:** Using the **Data Collector** to perform this scan is *Optional* if the unreachable computers are not to be a part of the HIPAA Assessment process.

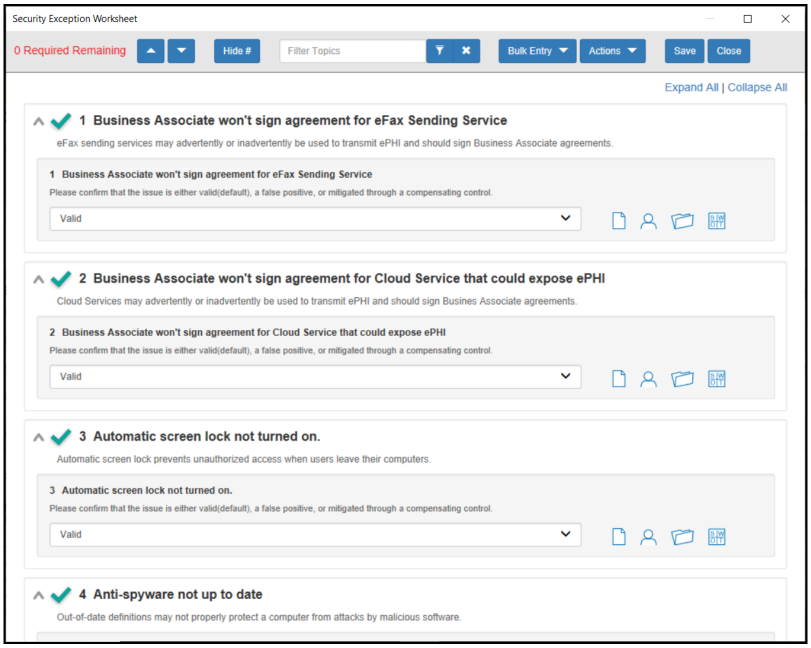
2. Complete the **Inactive Computer Identification Worksheet**.
3. Complete the **User Identification Worksheet**.
4. Complete the **Computer Identification Worksheet**.
5. Complete the **Network Share Identification Worksheet**.

Step 6 — Document Exceptions

Optional: Complete the **Security Exceptions Worksheet**.

The **Security Exception Worksheet** is an optional worksheet that compiles the issues discovered by the Push Deploy Tool Scans, HIPAA Data Collector, Surveys, and Assessment Worksheets used throughout the HIPAA assessment process to enable security exceptions to be specified along with compensating controls to manage the exceptions.

> **Tip:** Use the **Security Exception Worksheet** to handle "false positives" or explain why certain issues have been resolved. Your entries will affect the overall risk score and other areas in your assessment documentation.



1 Business Associate won't sign agreement for eFax Sending Service

eFax sending services may advertently or inadvertently be used to transmit ePHI and should sign Business Associate agreements.

1 Business Associate won't sign agreement for eFax Sending Service

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Valid

2 Business Associate won't sign agreement for Cloud Service that could expose ePHI

Cloud Services may advertently or inadvertently be used to transmit ePHI and should sign Busines Associate agreements.

2 Business Associate won't sign agreement for Cloud Service that could expose ePHI

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Valid

3 Automatic screen lock not turned on.

Automatic screen lock prevents unauthorized access when users leave their computers.

3 Automatic screen lock not turned on.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

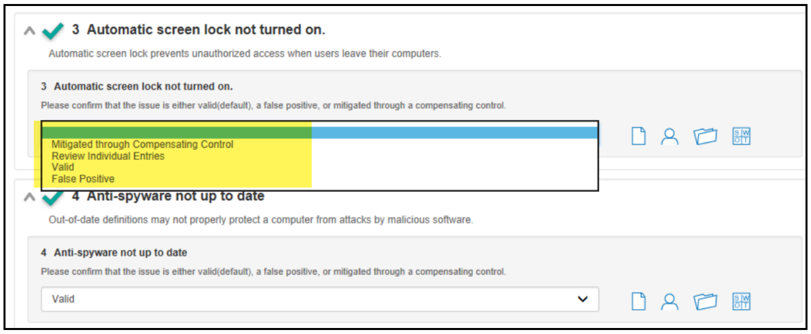
Valid

4 Anti-spyware not up to date

Out-of-date definitions may not properly protect a computer from attacks by malicious software.

To use the Security Exception Worksheet:

1. For each issue in the form, select one of the available options.



3 Automatic screen lock not turned on.

Automatic screen lock prevents unauthorized access when users leave their computers.

3 Automatic screen lock not turned on.

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Mitigated through Compensating Control
Review Individual Entries
Valid
False Positive

4 Anti-spyware not up to date

Out-of-date definitions may not properly protect a computer from attacks by malicious software.

4 Anti-spyware not up to date

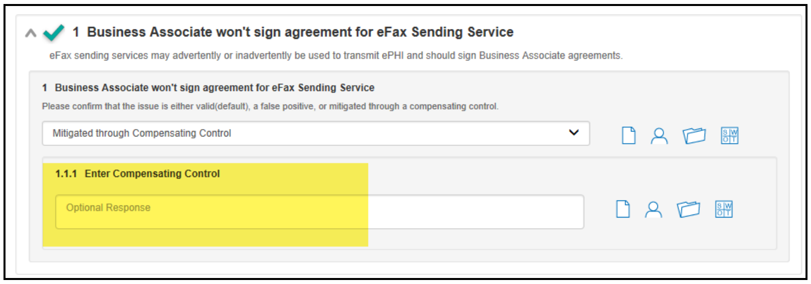
Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Valid

A. **Mitigated through Compensating Control**

i. Choose this option to enter a blanket response as to why all instances of the issue have been mitigated. For example, why do you not need signed agreements with your business associates that transmit ePHI?

ii. When you indicate that an issue has been mitigated, enter an **Optional Response** explaining how the issue has been resolved or why it's not relevant. These notes will appear in your final assessment documentation.



1 Business Associate won't sign agreement for eFax Sending Service

eFax sending services may advertently or inadvertently be used to transmit ePHI and should sign Business Associate agreements.

1 Business Associate won't sign agreement for eFax Sending Service

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

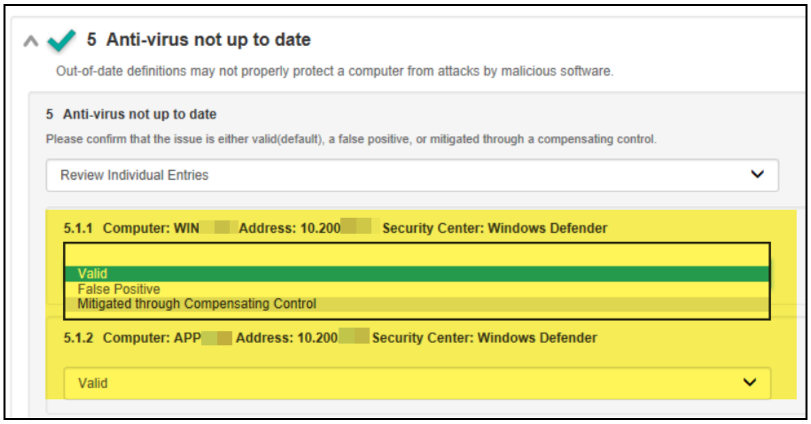
Mitigated through Compensating Control

1.1.1 Enter Compensating Control

Optional Response

B. **Review Individual Entries**

i. You can also choose to review each issue separately. This is useful if you need to explain why some of your PCs are detected as not having anti-virus or account lockout enabled, for example. When you choose to review individual entries, you can likewise indicate whether each entry is mitigated, valid, or a false positive.



5 Anti-virus not up to date

Out-of-date definitions may not properly protect a computer from attacks by malicious software.

5 Anti-virus not up to date

Please confirm that the issue is either valid(default), a false positive, or mitigated through a compensating control.

Review Individual Entries

5.1.1 Computer: WIN[redacted] Address: 10.200[redacted] Security Center: Windows Defender

5.1.2 Computer: APP[redacted] Address: 10.200[redacted] Security Center: Windows Defender

Valid

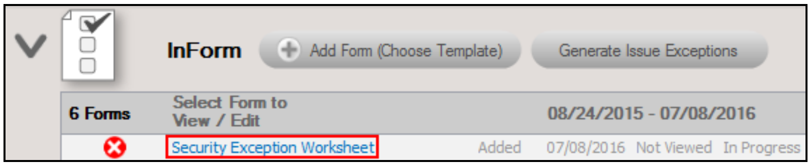
C. **Valid**: Indicates that the issue is valid and has not been addressed.

D. **False Positive**: Indicates that the issue is NOT valid and does not need to be addressed. Choose this option if you have trouble with the results from an automated scan, for example.

Important: Assessments completed and archived before 3/8/2019 will use the legacy Security Exception Worksheet. In order to access the new version of the worksheet:

1. Open your archived assessment.
2. Open the Security Exception Worksheet from your archived assessment.
3. Generate a Word Reports Form containing responses to maintain a record of the Security Exceptions documented using the legacy Security Exception Worksheet.
4. Delete the old Security Exception Worksheet.
5. A new Security Exception Worksheet will be generated in its place. Complete all required entries in the worksheet and proceed with your assessment.

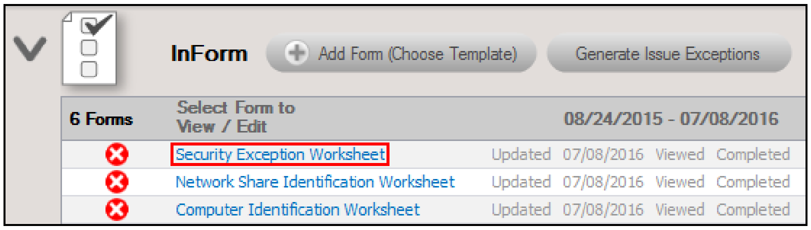
To open and complete the Security Exception Worksheet, click on the name label for the **Security Exception Worksheet** entry in the InForm Questionnaire/Worksheet list located below the InForm Bar at the bottom of the Assessment window.



6 Forms	Select Form to View / Edit	08/24/2015 - 07/08/2016			
☒	Security Exception Worksheet	Added	07/08/2016	Not Viewed	In Progress

Exceptions are grouped by a number of exception types that may include: Business Associate Agreements, Former Employee/Vendor Enabled Accounts, Remote Access Cloud Services, Firewall, Office Environment, Wireless, Endpoint Protection, and External Vulnerability Scan categories.

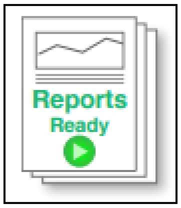
You can return to the Security Exception Worksheet by clicking on the name label located under the InForm Bar at the bottom of the Assessment Window.



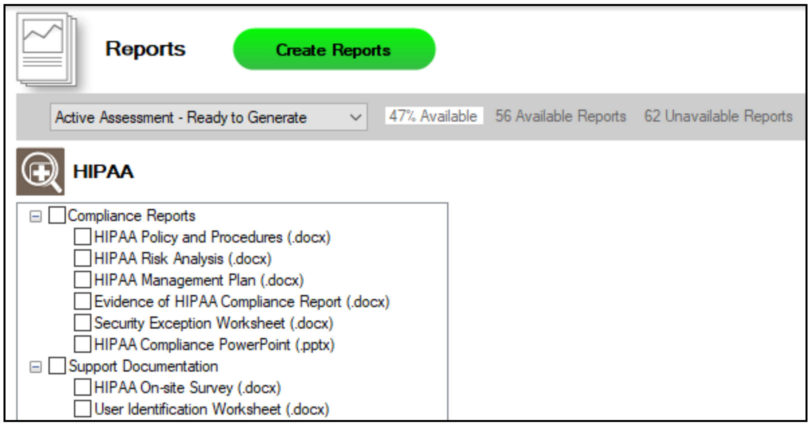
6 Forms	Select Form to View / Edit	08/24/2015 - 07/08/2016			
☒	Security Exception Worksheet	Updated	07/08/2016	Viewed	Completed
☒	Network Share Identification Worksheet	Updated	07/08/2016	Viewed	Completed
☒	Computer Identification Worksheet	Updated	07/08/2016	Viewed	Completed

Step 7 — Generate Reports

1. Run Network Detective and login with your credentials.
2. Then select the **Site** and go to the **Active Assessment Project**.
3. Click the Reports Ready button at the end of the assessment checklist.



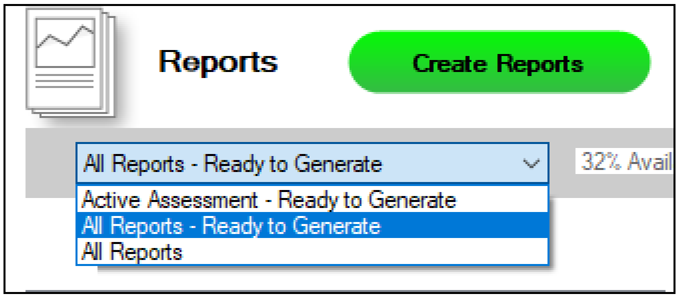
4. Select which of the HIPAA Compliance Assessment reports that you want to generate.



Active Assessment - Ready to Generate | 47% Available | 56 Available Reports | 62 Unavailable Reports

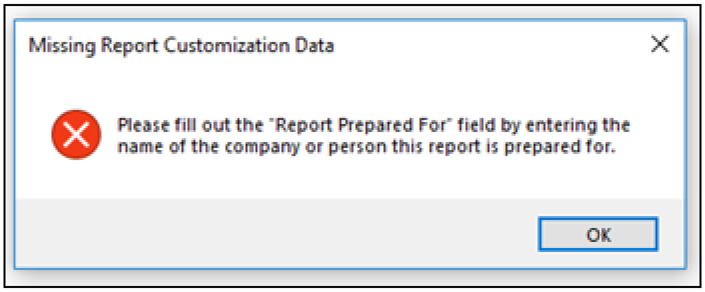
- ⊟ □ Compliance Reports
  - □ HIPAA Policy and Procedures (.docx)
  - □ HIPAA Risk Analysis (.docx)
  - □ HIPAA Management Plan (.docx)
  - □ Evidence of HIPAA Compliance Report (.docx)
  - □ Security Exception Worksheet (.docx)
  - □ HIPAA Compliance PowerPoint (.pptx)
- ⊟ □ Support Documentation
  - □ HIPAA On-site Survey (.docx)
  - □ User Identification Worksheet (.docx)

You can use the Reports drop-down menu to filter reports related to the active assessment project, reports that are ready to generate, or to browse all available reports.


Reports
Create Reports
All Reports - Ready to Generate
32% Avail
Active Assessment - Ready to Generate
All Reports - Ready to Generate
All Reports

5. Click the **Create Reports** button and follow the prompts to generate the reports you selected.

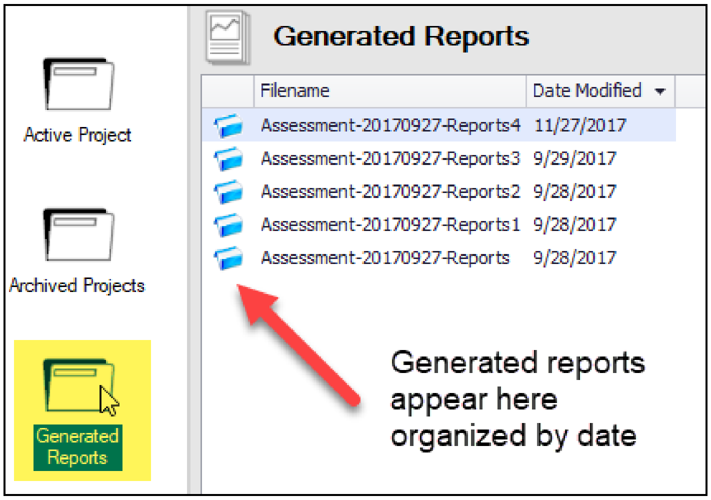
   i. If you have not previously edited your Report Preferences, you will be prompted to do so before generating reports.


Missing Report Customization Data

Please fill out the "Report Prepared For" field by entering the name of the company or person this report is prepared for.

Tip: See the [Network Detective User Guide]() for instructions on how to customize your reports with your company's branding.

Click **Generated Reports** from the left-hand Site menu to access previously generated reports. Double click a set of assessment reports to open the folder in Windows Explorer.



Generated Reports

Filename	Date Modified
Assessment-20170927-Reports4	11/27/2017
Assessment-20170927-Reports3	9/29/2017
Assessment-20170927-Reports2	9/28/2017
Assessment-20170927-Reports1	9/28/2017
Assessment-20170927-Reports	9/28/2017

Generated reports appear here organized by date

Note on Time to Generate Reports

Important: Larger data sets will require more time to generate reports. If the data set is especially large — in the range of several thousand users, for example — a full set of reports may take several hours to complete.

HIPAA Assessment Reports

The HIPAA Assessment Module can generate the following reports and supporting documents:

Compliance Reports

These reports show where you are in achieving HIPAA compliance. In addition, these documents identify and prioritize issues that must be remediated to address HIPAA related security vulnerabilities through ongoing managed services.

Report Name	Description
Evidence of HIPAA Compliance	Just performing HIPAA-compliant tasks is not enough. Audits and investigations require evidence that compliance tasks have been carried out and completed. Documentation must be kept for six years. The Evidence of Compliance includes log-in files, patch analysis, user & computer information, and other source material to support your compliance activities. When all is said and done, the proof to proper documentation is accessibility and the detail to satisfy an auditor or investigator included in this report.
HIPAA Compliance PowerPoint	Use our generated PowerPoint presentation as a basis for conducting a meeting presenting your findings from the Network Detective. General summary information along with the risk and issue score are presented along with specific issue recommendations and next steps.
HIPAA Management Plan	Based on the findings in the Risk Analysis, the organization must create a Risk Management Plan with tasks required to minimize, avoid, or respond to risks. Beyond gathering information, Network Detective provides a risk scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources and ensure that issues identified are issues solved. The Risk Management plan defines the strategies and tactics the organization will use to address its risks.
HIPAA Policies & Procedures	The Policy and Procedures are the best practices that our industry experts have formulated to comply with the technical requirements of the HIPAA Security Rule. The policies spell out what your organization will do while the procedures detail how

Report Name	Description
	you will do it. In the event of an audit, the first thing an auditor will inspect are the Policies and Procedures documentation. This is more than a suggested way of doing business. The Policies and Procedures have been carefully thought out and vetted, referencing specific code sections in the Security Rule and supported by the other reports include with the HIPAA Compliance module.
HIPAA Risk Analysis	HIPAA is a risk-based security framework and the production of a Risk Analysis is one of primary requirements of the HIPAA Security Rule's Administrative Safeguards. In fact, a Risk Analysis is the foundation for the entire security program. It identifies the locations of electronic Protected Health Information (ePHI,) vulnerabilities to the security of the data, threats that might act on the vulnerabilities, and estimates both the likelihood and the impact of a threat acting on a vulnerability. The Risk Analysis helps HIPAA Covered Entities and Business Associates identify the locations of their protected data, how the data moves within, and in and out of, the organization. It identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of ePHI. The value of a Risk Analysis cannot be overstated. Every major data breach enforcement of HIPAA, some with penalties over $1 million, have cited the absence of, or an ineffective, Risk Analysis as the underlying cause of the data breach. The Risk Analysis must be run or updated at least annually, more often if anything significant changes that could affect ePHI.
HIPAA Risk Profile	A Risk Analysis should be done no less than once a year. However, Network Detective has created an abbreviated version of the Risk Analysis called the HIPAA Risk Profile designed to provide interim reporting in a streamlined and almost completely automated manner. Whether performed monthly or quarterly, the Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks, and finds new ones that may have otherwise been missed and resulted in a data breach.
Security Exception Worksheet	The report is used present the details associated with security exceptions and how compensating controls will be or have been implemented to enable HIPAA compliance. This worksheet

Report Name	Description
	allows the HIPAA Compliance readiness specialist to document explanations on suspect items. The readiness specialist is enabled to document and explain why various discovered items are not true issues and possible false positives. These exceptions can be documented on an item by item level (for example: at the granularity at users, ports, applications, etc.). The Security Exception Worksheet compiles the issues discovered by the HIPAA Compliance Data Collection including the completion of the questionnaires and worksheets. The benefit of this feature is that it adds back in the human element into the assessment and allows for explanation of special circumstances and specific environment requirements. The Security Exception Worksheet does not alleviate the need for safe guards but allows for description of alternative means of mitigating the identified security risk. The process is consistent with industry standard HIPAA assessment and risk management processes

Supporting Documentation

These documents show the detailed information and raw data that backs up the compliance reports. These documents include the various interviews and worksheets, as well as detailed data collections on network assets, shares, login analysis, etc.

Report Type	Description
Computer Identification Worksheet	The Computer Identification Worksheet takes the list of computers gathered by the Data Collector and lets you identify those that store or access ePHI. This is an effective tool in developing data management strategies including secure storage and encryption. To save time the system allows you to enter default settings for all computers and just change some as needed. There is also an inactive computer identification worksheet.
Disk Encryption Report	Encryption is such an effective tool used to protect data that if an encrypted device is lost then it does not have to be reported as a data breach. The Disk Encryption Report identifies each drive and volume across the network, whether it is fixed or removable, and if Encryption is active.
External Network Vulnerability Scan Detail by Issue	Detailed reports showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.
File Scan Report	The underlying cause identified for many data breaches is that the organization did not know that protected data was stored on a device that was lost or stolen. After a breach of 4 million patient records a hospital executive said, "Based on our policies that data should not have been on those systems." The File Scan Report identifies data files stored on computers, servers, and storage devices. It does not read the files or access them, but just looks at the title and file type. This report is useful to identify local data files that may not be protected. Based on this information, the risk of a breach could be avoided if the data was moved to a more secure location, or mitigated by encrypting the device to protect the data and avoid a data breach investigation.
HIPAA On-Site Survey	The On-site Survey is an extensive list of questions about physical and technical security that cannot be gathered automatically. The survey includes questions ranging from how

Report Type	Description
	facility doors are locked, firewall information, how faxes are managed, and whether servers are on-site, in a data center, or in the Cloud.
Inactive Computer Identification Worksheet	In this worksheet you identify computers that are detected as inactive for a long period of time. Such computers pose a potential data risk as they are likely not managed and/or secured.
Login History by Computer Report	Same data as User Behavior but inverted to show you by computer. Quite useful, in particular, for looking at a commonly accessed machines (file server, domain controller, etc.) – or a particularly sensitive machine for failed login attempts. An example would be CEO's laptop – or the accounting computer where you want to be extra diligent in checking for users trying to get in.
Network Share Identification Worksheet	The Network Share Identification Worksheet takes the list of network shares gathered by the Data Collector and lets you identify those that store or access ePHI. This is an effective tool in developing data management strategies including secure storage and encryption. To save time the system allows you to enter default settings for all network shares and just change some as needed
Share Permission Report	Comprehensive lists of all network "shares" by computer, detailing which users and groups have access to which devices and files, and what level of acfcess they have.
User Identification Worksheet	The User Identification Worksheet takes the list of users gathered by the Data Collector and lets you identify whether they are an employee or vendor. Users who should have been terminated and should have had their access terminated can also be identified. This is an effective tool to determine if unauthorized users have access to protected information. It also is a good indicator of the efforts the organization goes to so terminated employees and vendors have their access quickly disabled. Another benefit is that you can review the user list to identify generic log-ons, such as Nurse, Billing Office, etc., which are not allowed by HIPAA since each user is required to be uniquely identified. To save time the system allows you to enter default settings for all users and just change some as needed.

Change Reports

Report Name	Description
Baseline HIPAA Management Plan	The Risk Management plan defines the strategies and tactics the organization will use to address its risks.
Baseline HIPAA Risk Profile	The Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks.