Compliance HIPPA Health Insurance Portability and Accountability Act

Manage everything associated with HIPAA's Security Rule. This module is designed to be used by any HIPAA "Covered Entity" (any organization in the healthcare industry) as well as any "Business Associate" (any company that works with a Covered Entity that may have physical or electronic access to patient information. It includes everything you need to automatically generate evidence of compliance in the event of an audit.

Compliance Process Automation for HIPAA

HIPAA Manager provides a step-by-step framework to help you tackle HIPAA audits and compliance services. We have taken the guess work out of compliance-as-a-service by automating the production of mandatory reporting under HIPAA. Our solution will look at the results of the manual surveys and worksheets and compare it to data from our automated scanning to uncover HIPAA related network issues, policy flaws, and potential breaches

Primary Documents

HIPAA Evidence of Compliance

Compiles compliance information from both automated scans, augmented data, and questionnaires. Gathers evidence into one document to back up the HIPAA Security Rule Auditor Checklist with real data.

HIPAA Risk Analysis

The HIPAA Risk Analysis is the foundation for the entire HIPAA compliance and IT security program. The HIPAA Risk Analysis 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 at rest and/or during its transmission.

HIPAA Management Plan

Based on the findings in the HIPAA Compliance Assessment, the organization must create a HIPAA Management Plan with tasks required to minimize, avoid, or respond to risks. Beyond gathering information, HIPAA Manager 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 HIPAA Management Plan defines the strategies and tactics the organization will use to address its risks.

HIPAA Policies and Procedures

One of the first requirements is to have a set of policies and procedures used to implement ePHI data security and compliance with HIPAA. Some organizations don't have a set of data protection policies – or at least one that conforms to HIPAA provisions. The tool provides an "out of the box" version of policies and procedures for

HIPAA for use by those organizations.

HIPAA Auditor Checklist The HIPAA Auditor Checklist gives you a high-level overview of how well the organization complies with the HIPAA provisions. The checklist details specific compliance items, their status, and helpful references. Use the checklist to quickly identify potential issues to be remediated in order to achieve compliance.

HIPAA Breach Notification Rule Worksheet

The HIPAA Breach Notification Rule Worksheet enables the Covered Entity to assess how well its organization's policies and procedures adhere to the HIPAA Breach Notification Rule requirements.

HIPAA Privacy Rule Worksheet

The HIPAA Privacy Rule Worksheet enables the Covered Entity to assess how well its organization's policies and procedures adhere to the HIPAA Privacy Rule requirements.

Supporting Documents

HIPAA Security Exceptions Worksheet

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.

HIPAA Compliance PowerPoint Use the generated PowerPoint presentation as a basis for conducting a meeting presenting your findings from the HIPAA Manager assessment process. General summary information along with the risk and issue score are presented along with specific issue recommendations and next steps.

Network Share Identification Worksheet

The Network Share Identification Worksheet takes the list of network shares gathered by the Data Collection process 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.

HIPAA Drive Encryption Worksheet

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.

HIPAA External Vulnerability Scan Detail by Issue

Detailed report 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.

HIPAA ePHI Validation Worksheet

During the ePHI scan performed by HIPAA Manager, suspected ePHI may be detected in files stored on network and stand-alone computers. The ePHI Validation Worksheet report presents a record of which computer files were verified by a participant in the HIPAA assessment process as containing actual instances of ePHI.

HIPAA ePHI Scan System Selection Worksheet

Understanding where you have ePHI Data is an important component of HIPAA compliance. The Personal Data Scan System Selection Worksheet allows you to specify which systems are scanned for ePHI during the assessment process. A comprehensive scan should be performed annually to help identify and document all potential locations for personal data as defined by HIPAA.

HIPAA On-Site Survey

Assess the physical security and the workplace environment as it relates to information security. The worksheet will guide you through your assessment of the physical security. This worksheet includes information about the Information Security Officer. It is best done on-site as it requires identifying risk that may currently exist in the client's environment outside the computer network itself.

HIPAA Policies and Procedures Verification Worksheet

The HIPAA Policy and Procedures Verification Worksheet will collect information about the network and environment that cannot be discovered through automated scans. This includes information principles relating to processing of ePHI, including sanctions, incident response, and Business Associates of the Covered Entity.

HIPAA Computer Identification Worksheet

The Computer Identification Worksheet is used to augment the asset data that was collected during the internal network scan. Details include the Device Name, Device Type, IP Address, Operating System, System Description, as well as device and sensitive information classification. The ePHI Access Classification is used to determine the risk to the organization in the event of a security incident where the asset's information is compromised.

HIPAA User Identification Worksheet

The User Identification Worksheet is used to augment the user data that was collected during the internal network scan. Complete the worksheet to provide the additional information requested.

HIPAA External Port Use Worksheet

This worksheet allows you to document business justifications for all of the allowed external ports, the protocol configured to use a specific port, and the documentation of any insecure configurations implemented and in use for a given protocol.

HIPAA Risk Update Assessment Reports

HIPAA External Vulnerability Scan Detail Detailed report 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.

HIPAA Risk Management Plan Update

Based on the findings in the HIPAA Risk Update Assessment, the organization must create a HIPAA Management Plan with tasks required to minimize, avoid, or respond to identified risk to IT security and HIPAA regulatory compliance.

The HIPAA Management Plan Update report contains a list of tasks that can be executed to mitigate identified IT Security risks and HIPAA compliance lapses.

HIPAA Change Summary Report Every time you use HIPAA Manager to run a HIPAA Risk Update assessment on a given network, the HIPAA Manager generates the HIPAA Change Summary report.

This report compares the results the last Full HIPAA Assessment with the Risk Update Assessment's network scan, local computer scan(s), and external vulnerability scan results performed during the Risk Update Assessment process.

This report details changes in the network's User Accounts, Local Computer Accounts, Active Directory (A/D) Computers, Non-A/D Computers, Non-A/D Devices, External Vulnerabilities, along with a Windows computer Patch Summary.

HIPAA Risk Analysis Update

HIPAA Risk Analysis Update report lists IT Security risks identified during a Risk Update Assessment that impact the state of network security and HIPAA compliance. The HIPAA Risk Analysis Update identifies what protections are in place and where there is a need for more.

The HIPAA Risk Analysis Update report presents results in a list of items that must be remediated to ensure the security and confidentiality of ePHI at rest and/or during its transmission.