advanced
data & network solutions

HIPAA Assessment

HIPAA Risk Analysis

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared by:
Advanced Data
Prepared for:
Anonymous

Table of Contents

Overview

Risk management, required by the HIPAA Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of ePHI and protect against any reasonably anticipated threats, hazards, or disclosures of ePHI not permitted or required under HIPAA.

After a Risk Analysis the next step in the risk management process is to develop and implement a Risk Management Plan. The purpose of a Risk Management Plan is to provide structure for the evaluation, prioritization, and implementation of risk-reducing measures and controls.

Risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their "risk score." The implementation components of the plan include:

- Risk score (threat and vulnerability combinations) assigned to a particular issue being addressed;
- Recommendation(s) of measures and controls selected to reduce the risk of an issue;
- Ongoing evaluation and monitoring of the risk mitigation measures.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Risk Score

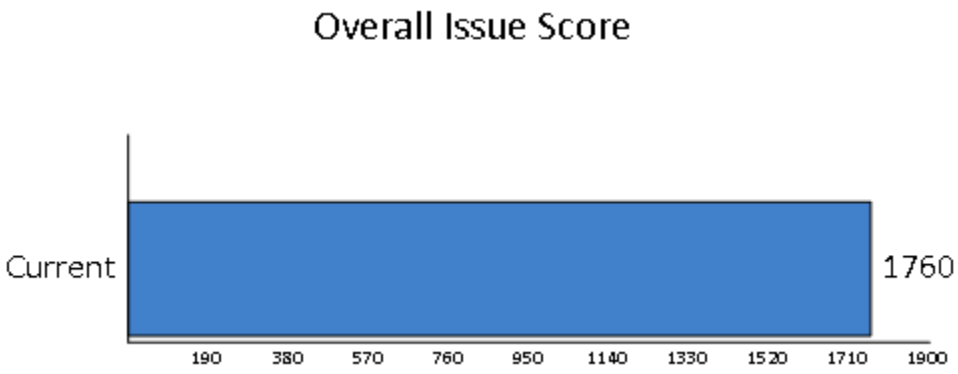
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues.

Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

If additional information is needed, please consult the Evidence of HIPAA Compliance.

Issues Summary

This section contains a summary of issues detected during the Network Assessment process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Unsupported Operating Systems (90 pts)

Issue: 6 computers were found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.
Recommendation: Upgrade or replace computers with operating systems that are no longer supported.

User has not logged in in 30 days (10 pts)

Issue: Users that have not logged in in 30 days could be from a former employee or vendor and should be disabled or removed.
Recommendation: Disable or remove user accounts for users that have not logged in in 30 days.

User password set to never expire (80 pts)

Issue: User accounts with passwords set to never expire present a risk of use by authorized users. They are more easily compromised than passwords that are routinely changed.
Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

Non-administrative generic logons have access to Network Share on system with ePHI (80 pts)

Issue: Generic accounts which could be in use by multiple people cannot be properly restricted and should not have access to network shares with ePHI.
Recommendation: Remove access to Network Shares on systems with ePHI.

Password complexity not enabled (70 pts)

Issue: Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.
Recommendation: Enable password complexity to assure domain account passwords are secure.

Automatic screen lock not turned on. (90 pts)

Issue: Automatic screen lock prevents unauthorized access when users leave their computers.
Recommendation: Enable automatic screen lock on the following computers: DC01

Computer with ePHI does not have object level auditing on (10 pts)

Issue: Object level auditing helps identify users who have accessed files and other system resources. Object level auditing may impose an unacceptable performance impact and should be considered for use on high risk computers or environments.
Recommendation: Evaluate the pros and cons of enabling object level access or ensure alternative methods for breach identification are in place.

Significantly high number of Domain Administrators (30 pts)

Issue: More than 30% of the users are in the Domain Administrator group and have unfettered access to files and system resources. Compromised Domain Administrator accounts pose a higher threat than typical users and may lead to a breach.
Recommendation: Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary.

Computers are in Workgroup Environment (30 pts)

Issue: Isolated computers and computers in a workgroup environment cannot take advantage of auditing and access controls provided by a domain. They inherently increase the risk of breach and should be discouraged. Alternative means of protection must be employed to ensure computers in a workgroup are properly protected.
Recommendation: Migrate computers into a Domain environment.

Password history not remembered for at least 6 passwords (70 pts)

Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.
Recommendation: Increase password history to remember at least 6 passwords.

Account lockout disabled (70 pts)

Issue: Account lockout (disabling an account after a number of failed attempts) significantly reduces the risk of an attacker acquiring a password through a brute force attack.
Recommendation: Enable account lockout for all users.

Audit user login in not turned on (30 pts)

Issue: Login auditing is required for proper identification of access to computers and resources. In the event of a breach, audit logs can be used to identify unauthorized access and the severity of the breach.
Recommendation: Enable user login auditing.

Anti-virus not installed (90 pts)

Issue: Malware protection is required but not identified as being installed on computers in the network.
Recommendation: Install a commercial grade anti-virus program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.

Anti-virus not turned on (90 pts)

Issue: Malware protection is required but not identified as being enabled on computers in the network.
Recommendation: Enable anti-virus program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.

Anti-virus not up to date (90 pts)

Issue: Out-of-date definitions may not properly protect a computer from attacks by malicious software.
Recommendation: Ensure anti-virus programs on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report are up-to-date.

Anti-spyware not installed (90 pts)

Issue: Malware protection is required but not identified as being installed on computers in the network.
Recommendation: Install a commercial grade anti-spyware program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.

Anti-spyware not turned on (90 pts)

Issue: Malware protection is required but not identified as being enabled on computers in the network.
Recommendation: Enable anti-spyware program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.

Anti-spyware not up to date (90 pts)

Issue: Out-of-date definitions may not properly protect a computer from attacks by malicious software.
Recommendation: Ensure anti-spyware programs on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report are up-to-date.

USB drives detected in use (50 pts)
Issue: The use of USB drives increase the change of data loss through theft and should be discouraged to the extent possible.
Recommendation: Reduce or eliminate the use of USB drives in the environment.

Workstations with ePHI not backed up (70 pts)
Issue: Security Center reports that computers identified as having ePHI are not backed up.
Recommendation: Ensure that data is properly backed up on computers with ePHI. See the Endpoint Security section of the Evidence of HIPAA Compliance for a list of computers.

Firewall does not have malware filtering (10 pts)
Issue: Firewall malware filtering is recommended for increase protection against malicious software.
Recommendation: Enable malware filtering on firewalls or investigate putting in place a firewall with malware filtering services.

Inconsistent password policy / Exceptions to password policy (70 pts)
Issue: Password policies are not consistently applied from one computer to the next. A consistent password policy ensure adherence to password best practices.
Recommendation: Eliminate inconsistencies and exceptions to the password policy.

User marked as not requiring ePHI has access to network share with ePHI (80 pts)
Issue: Network shares that contain ePHI should not allow read or write permissions to users that are marked as not having ePHI access.
Recommendation: Remove access to network shares identified as having ePHI from users marked as not requiring ePHI access.

Terminated employee account enabled (90 pts)
Issue: One or more accounts are still enabled for terminated employees. This poses a risk of unauthorized access.
Recommendation: Disable accounts for all terminated employees.

Terminated vendor account enabled (90 pts)
Issue: One or more accounts are still enabled for terminated vendors. This poses a risk of unauthorized access.
Recommendation: Disable accounts for all terminated vendors.

User not logged in in 90 days (not terminated) (20 pts)
Issue: Inactive user accounts were found that could potentially indicate terminated employees or vendors.
Recommendation: Investigate all inactive accounts and disable accounts from terminated employees and vendors.

Unrestricted network share with ePHI (80 pts)

Issue: Network shares containing ePHI were found as completely unrestricted (granting access to 'Everyone').

Recommendation: Investigate the network shares containing ePHI with unrestricted access. Limit access to the minimum necessary.