HIPAA Assessment
HIPAA Risk Analysis Update

Prepared for:

HIPAA - Covered Entity

Prepared by:

AMS Networks

Scan Date: 01-Oct-2019

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.

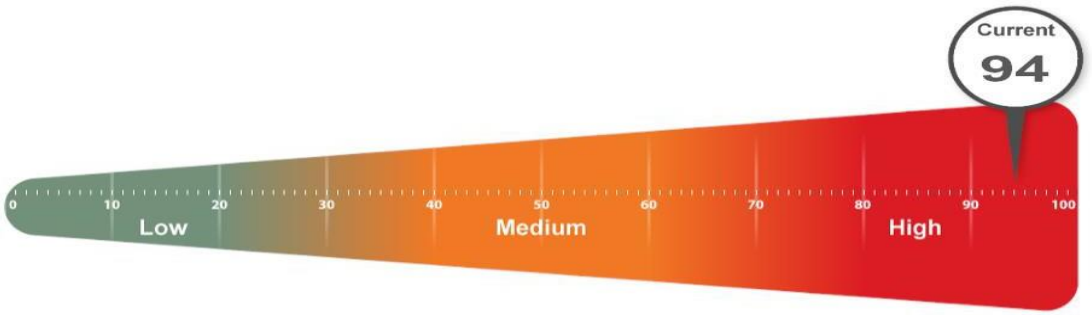
Risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their "risk score." The implementation components of the plan include:

- 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 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.

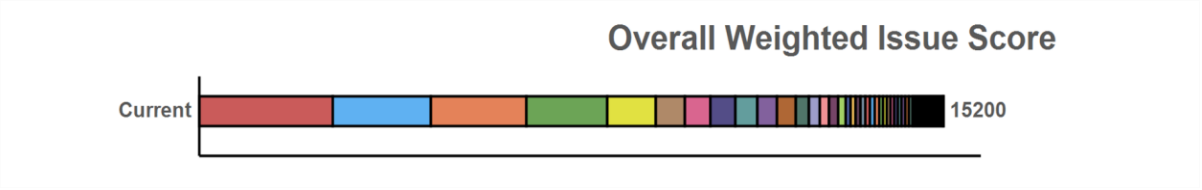


Several critical issues were identified. Identified issues should be investigated and addressed according to the HIPAA Management Plan Update report.

If additional information is needed on how the risk score was determined, please perform a full HIPAA assessment and consult the Evidence of Compliance report produced from the assessment.

Issues Summary

This section contains a summary of issues detected during the HIPAA 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.



Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

	Automatic screen lock not turned on (94 pts each)
2726	***Current Score:*** 94 pts x 29 = 2726: 17.93%
	Requirement: §164.312(a)(1) Access Control - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
	Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.
	Recommendation: Enable automatic screen lock on the specified computers.

	Account lockout disabled (77 pts each)
2002	***Current Score:*** 77 pts x 26 = 2002: 13.17%
	Requirement: §164.308(a)(5)(ii)(d): Password Management - Procedures for creating, changing, and safeguarding passwords.
	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.

	Passwords less than 8 characters allowed (75 pts each)
1950	***Current Score:*** 75 pts x 26 = 1950: 12.83%
	Requirement: §164.308(a)(5)(ii)(d): Password Management - Procedures for creating, changing, and safeguarding passwords.
	Issue: Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.
	Recommendation: Enable enforcement of password length to more than 8 characters.

	Lots of Security patches missing on computers (90 pts each)
990	***Current Score:*** 90 pts x 11 = 990: 6.51%
	Requirement: §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.

	Issue: Security patches are missing, maintaining proper security patch levels is required by HIPAA to prevent unauthorized access and the spread of malicious software. Lots is defined as missing 3 or more patches and may be an indicator of issues with the patching system.
	Recommendation: Address patching on computers missing 4+ security patches.

	Significantly high number of Domain Administrators (35 pts each)
595	***Current Score:*** 35 pts x 17 = 595: 3.91%
	Requirement: 45 CFR §164.308(A)(3) - Standard Workforce Security - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
	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.

	User password set to never expire (30 pts each)
510	***Current Score:*** 30 pts x 17 = 510: 3.36%
	Requirement: §164.308(A)(5)(ii)(D): Password Management - Procedures for creating, changing, and safeguarding passwords.
	Issue: User accounts with passwords set to never expire present a risk of use by unauthorized 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.

	Anti-virus not up to date (90 pts each)
450	***Current Score:*** 90 pts x 5 = 450: 2.96%
	Requirement: §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.
	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.

	User not logged in in 90 days (not terminated) (25 pts each)
400	***Current Score:*** 25 pts x 16 = 400: 2.63%
	Requirement: §164.308(a)(3)(ii)(C): - Termination Procedures - Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in a)(3)(ii)(B) of this section.
	Issue: Inactive user accounts were found that could potentially indicate terminated employees or vendors.
	Recommendation: Disable or remove user accounts for users that have not logged on to

active directory in 90 days.

	Terminated employee account enabled (96 pts each)
384	***Current Score:*** 96 pts x 4 = 384: 2.53%
	Requirement: §164.308(A)(3)(ii)(C): - Termination Procedures - Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in a)(3)(ii)(B) of this section.
	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.

	Medium External Vulnerabilities Detected (75pts each)
300	***Current Score:*** 75pts x4 = 300: 8.99%
	Requirement: §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedures for guarding against, detecting, and reporting malicious software.
	Issue: Medium severity external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
	Recommendation: Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.

	Anti-spyware not up to date (90 pts each)
270	***Current Score:*** 90 pts x 3 = 270: 1.78%
	Requirement: §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.
	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.

	User has not logged on to domain in 30 days (13 pts each)
221	***Current Score:*** 13 pts x 17 = 221: 1.45%
	Requirement: §164.308(A)(3)(ii)(C): - Termination Procedures - Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in a)(3)(ii)(B) of this section.
	Issue: Users have not logged on to domain in 30 days. A user that has not logged in for an extended period of time could be a former employee or vendor.
	Recommendation: Disable or remove user accounts for users that have not logged on to active directory in 30 days.

	Anti-spyware not installed (94 pts each)
188	***Current Score:*** 94 pts x 2 = 188: 1.24%
	Requirement: §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for

	guarding against, detecting, and reporting malicious software.
	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-virus not installed (94 pts each)
188	***Current Score:*** 94 pts x 2 = 188: 1.24%
	Requirement: §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.
	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.

	Computer with ePHI does not have object level auditing on (11 pts each)
154	***Current Score:*** 11 pts x 14 = 154: 1.01%
	Requirement: §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
	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.

	Audit user login in not turned on (30 pts each)
30	***Current Score:*** 30 pts x 1 = 30: 0.2%
	Requirement: §164.308(a)(1)(ii)(D): Information System Activity Review - Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security tracking reports.
	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.

	Use of generic logins (1 pts each)
5	***Current Score:*** 1 pts x 5 = 5: 0.03%
	Requirement: §164.308(a)(1)(ii)(D): Information System Activity Review - Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security tracking reports.
	Issue: While not inherently a risk, the use of generic logins (logins used by more than one person or anonymous individuals) should be discouraged.
	Recommendation: Evaluate the necessity of generic logins and reduce their use when possible.