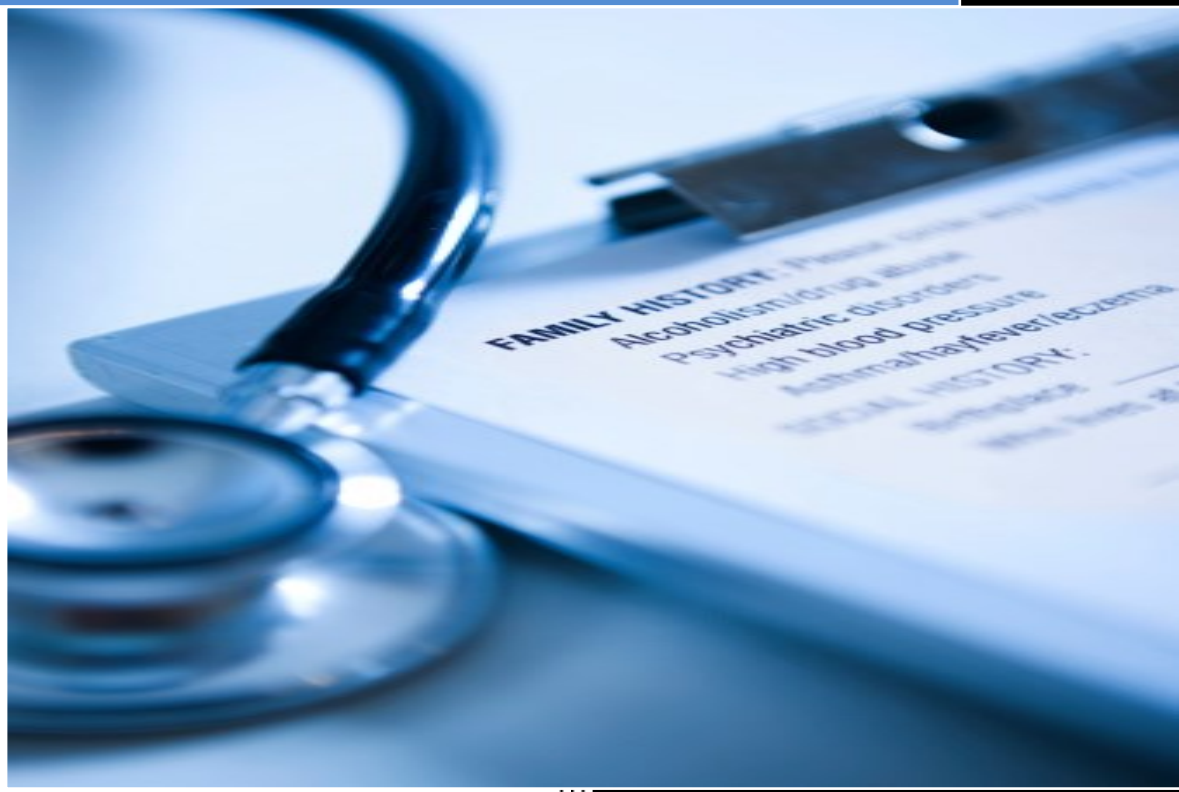
YourIT!
Your Logo Goes Here

# HIPAA Assessment

## HIPAA Risk Analysis






Scan Date: 13-Dec-2018

Prepared for:
HIPAA – Covered Entity
Prepared by:
YourIT Company

14-Dec-2018

# 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.

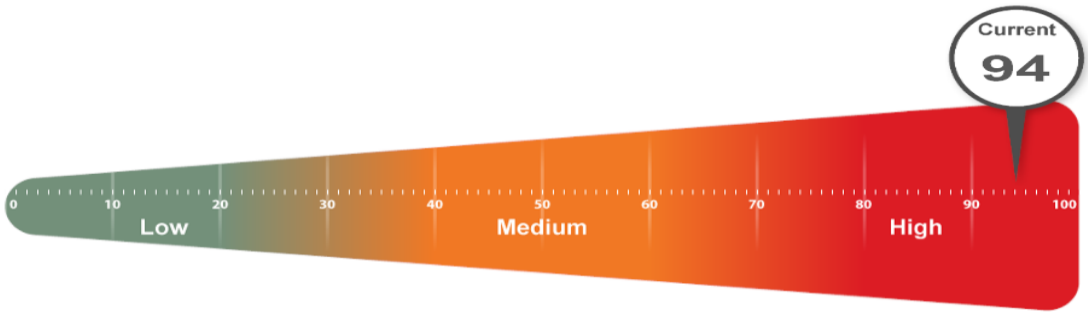
Risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their "risk score." The implementation components of the plan include:

- 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.

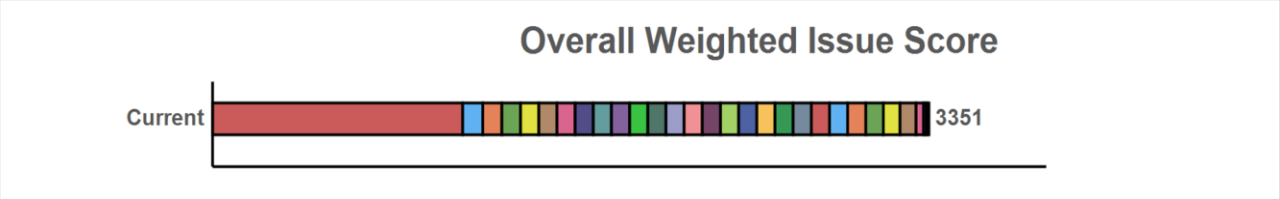



Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

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

# Issues Summary

This section contains a summary of issues detected during the 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 (%)

| | |
|---|---|
| | **Lots of Security patches missing on computers with ePHI (90 pts each)** |
| 1170 | ***Current Score:*** 90 pts x 13 = 1170: 34.91% |
| | ***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 on computers designated as having ePHI. 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. |

| | |
|---|---|
| | **Automatic screen lock not turned on (94 pts each)** |
| 94 | ***Current Score:*** 94 pts x 1 = 94: 2.81% |
| | ***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. |

| | |
|---|---|
| | **Missing or inadequate Business Associates Agreements. (89 pts each)** |
| 89 | ***Current Score:*** 89 pts x 1 = 89: 2.66% |
| | ***Requirement:*** §164.308(b)(1): Business Associate Contracts and Other Arrangements - Covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in $160.103. The covered entity must obtain satisfactory assurance from the business associate that it will appropriately safeguard the information in accordance with §164.314(a)(1) standards. |
| | ***Issue:*** Organizations are required to have signed Business Associates Agreements with all vendors who may have access to ePHI. The agreement must meet the requirements of the 2013 HIPAA Omnibus Final Rule. |

| | |
|---|---|
| | ***Recommendation:*** Create or modify the existing Business Associates Agreements to comply with the 2013 HIPAA Omnibus Final Rule. |

| | **Missing written Application Data and Criticality Analysis. (88 pts each)** |
|---|---|
| 88 | ***Current Score:*** 88 pts x 1 = 88: 2.63% |
| | ***Requirement:*** §164.308(a)(7)(i): Contingency plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. (ii) Implementation specifications: (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data. (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. (D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans. (E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components |
| | ***Issue:*** Organizations are required to perform an analysis of application data and criticality. |
| | ***Recommendation:*** Perform an analysis of application data and criticality. Use the analysis to properly implement safeguards that protect critical data. |

| | **Missing written ePHI Transmission Encryption Procedure. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.312(e)(1): Transmission Security – Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. |
| | ***Issue:*** Organizations are required to have a written procedure to protect and encrypt ePHI during transmission. |
| | ***Recommendation:*** Create a written procedure to protect and encrypt ePHI during transmission. |

| | **Missing written ePHI transmission Integrity Control Procedure. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.312(e)(1): Transmission Security – Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. |
| | ***Issue:*** Organizations are required to have a written procedure for maintaining Integrity Controls used during transmission of ePHI. |
| | ***Recommendation:*** Create a written procedure for maintaining Integrity Controls used during transmissions of ePHI and share it with the individuals responsible for its implementation. |

| | **Missing written Emergency Access Procedure. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |

| | |
|---|---|
| | ***Requirement:*** §164.312(c)(1): Integrity - Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. |
| | ***Issue:*** Organizations are required to have a written procedure to protect the Integrity of Data Against Improper Alteration and Destruction. |
| | ***Recommendation:*** Create a written procedure to protect the Integrity of Data Against Improper Alteration and Destruction and share it with the individuals responsible for its implementation. |

| | **Missing written Emergency Access Procedure. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***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:*** Organizations are required to have a written Emergency Access Procedure. |
| | ***Recommendation:*** Create a written Emergency Access Procedure and share it with the individuals responsible for its implementation. |

| | **Missing written Data Backup and Storage Procedure. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. |
| | ***Issue:*** Organizations are required to have a written Data Backup and Storage Procedure. |
| | ***Recommendation:*** Create a written Data Backup and Storage Procedure and share it with the individuals responsible for its implementation. |

| | **Missing written Media Accountability Policy. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. |
| | ***Issue:*** Organizations are required to have a written Media Accountability Policy. |
| | ***Recommendation:*** Create a written Media Accountability Policy and share it with the individuals responsible for its implementation. |

| | **Missing written Media Reuse Policy. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these |

| | |
|---|---|
| | items within the facility. |
| | ***Issue:*** Organizations are required to have a written Media Reuse Policy. |
| | ***Recommendation:*** Create a written Media Reuse Policy and share it with the individuals responsible for its implementation. |

| | **Missing written Media Disposal Policy. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. |
| | ***Issue:*** Organizations are required to have a written Media Disposal Policy. |
| | ***Recommendation:*** Create a written Media Disposal Policy and share it with the individuals responsible for its implementation. |

| | **Missing written Workstation Security Procedure. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.310(c): Workstation security - Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. |
| | ***Issue:*** Organizations are required to have a written Workstation Security Procedure. |
| | ***Recommendation:*** Create a written Workstation Security Procedure and share it with the individuals responsible for its implementation. |

| | **Missing written Workstation Use Policy (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.310(b): Workstation use - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. |
| | ***Issue:*** Organizations are required to have a written Workstation Use Policy that is shared with your workforce members. |
| | ***Recommendation:*** Create a written Workstation Use Policy and share it with your workforce members. |

| | **Missing written Access Control and Validation Procedure. (85 pts each)** |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. |
| | ***Issue:*** Organizations are required to have a written Access Control and Validation Procedure. |
| | ***Recommendation:*** Create a written Access Control and Validation Procedure and share it with the individuals responsible for its implementation. |

| | |
|---|---|
| | **Missing written Facility Security Plan. (85 pts each)** |
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. |
| | ***Issue:*** Organizations are required to have a written Facility Security Plan. |
| | ***Recommendation:*** Create a written Facility Security Plan and share it with the individuals responsible for its implementation. |

| | |
|---|---|
| | **Missing evidence of ongoing monitoring and planning to evaluate security plans and procedures. (85 pts each)** |
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.308(a)(8): Evaluation - Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart. |
| | ***Issue:*** Organizations are required to implement ongoing monitoring and planning to evaluate security plans and procedures to adequately protect ePHI. |
| | ***Recommendation:*** Implement ongoing monitoring and planning to evaluate security plans and procedures to adequately protect ePHI. |

| | |
|---|---|
| | **Missing written Contingency Plan (85 pts each)** |
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.308(a)(7)(i): Contingency plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. (ii) Implementation specifications: (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data. (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. (D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans. (E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components §164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. |
| | ***Issue:*** Organizations are required to have a written Contingency Plan. |
| | ***Recommendation:*** Create a written Contingency Plan and share it with the individuals responsible for its implementation. |

| | |
|---|---|
| | **Missing written Emergency Mode Operations Plan (85 pts each)** |

| | |
|---|---|
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.308(a)(7)(i): Contingency plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. (ii) Implementation specifications: (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data. (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. (D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans. (E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components |
| | ***Issue:*** Organizations are required to have a written Emergency Mode Operations Plan. |
| | ***Recommendation:*** Create a written Emergency Mode Operations Plan and share it with the individuals responsible for its implementation. |

| | |
|---|---|
| | **Missing written Disaster Recovery Plan (85 pts each)** |
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.308(a)(7)(i): Contingency plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. (ii) Implementation specifications: (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data. (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. (D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans. (E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components |
| | ***Issue:*** Organizations are required to have a written Disaster Recovery Plan. |
| | ***Recommendation:*** Create a written Disaster Recovery Plan and share it with the individuals responsible for its implementation. |

| | |
|---|---|
| | **Missing written Security Incident Response and Reporting Plan (85 pts each)** |
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.308(a)(6)(i): Security incident procedures - Implement policies and procedures to address security incidents. Missing written Security Incident Response and Reporting Plan. |
| | ***Issue:*** Organizations are required to have a written Security Incident Response and Reporting Plan. |
| | ***Recommendation:*** Create a written Security Incident Response and Reporting Plan and share it with the individuals responsible for its implementation. |

| | |
|---|---|
| | **Missing written Access Policy (85 pts each)** |
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information<br>for example, through access to a workstation, transaction, program, process, or other mechanism. |
| | ***Issue:*** Organizations are required to have a written procedure to establish and modify access. |
| | ***Recommendation:*** Create a written Access Policy and share it with the individuals responsible for its implementation. |

| | |
|---|---|
| | **Missing written Sanction Policy (85 pts each)** |
| 85 | ***Current Score:*** 85 pts x 1 = 85: 2.54% |
| | ***Requirement:*** §164.308(a)(1)(ii)(C): Sanction policy - Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. |
| | ***Issue:*** Organizations are required to have a written Sanction Policy that is shared with your workforce members. |
| | ***Recommendation:*** Create a written Sanction Policy and share it with your workforce members. |

| | |
|---|---|
| | **Missing written procedure for maintaining Facility Access Control maintenance records. (82 pts each)** |
| 82 | ***Current Score:*** 82 pts x 1 = 82: 2.45% |
| | ***Requirement:*** §164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. |
| | ***Issue:*** Organizations are required to have a written procedure for maintaining Facility Access Control maintenance records. |
| | ***Recommendation:*** Create a written procedure for maintaining Facility Access Control maintenance records and share it with the individuals responsible for its implementation. |

| | |
|---|---|
| | **Workstations with ePHI not backed up (78 pts each)** |
| 78 | ***Current Score:*** 78 pts x 1 = 78: 2.33% |
| | ***Requirement:*** §164.308(A)(7)(ii)(A) - Data Backup Plan - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. §164.308(A)(7)(ii)(B) - Disaster Recovery Plan - Establish (and implement as needed) procedure to restore any loss of data. |
| | ***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. |

| | |
|---|---|
| | **Medium External Vulnerabilities Detected (75 pts each)** |
| 75 | ***Current Score:*** 75 pts x 1 = 75: 2.24% |

| | |
|---|---|
| | ***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 remediating all external vulnerabilities as prescribed. |

| | **Significantly high number of Domain Administrators (35 pts each)** |
|---|---|
| 35 | ***Current Score:*** 35 pts x 1 = 35: 1.04% |
| | ***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. |

| | **Firewall does not have malware filtering (14 pts each)** |
|---|---|
| 14 | ***Current Score:*** 14 pts x 1 = 14: 0.42% |
| | ***Requirement:*** §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software. |
| | ***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. |

| | **Computer with ePHI does not have object level auditing on (11 pts each)** |
|---|---|
| 11 | ***Current Score:*** 11 pts x 1 = 11: 0.33% |
| | ***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. |