HIPAA Assessment

HIPAA Risk Analysis

Scan Date: 13-Dec-2018

Prepared for:
HIPAA – Covered Entity
Prepared by:
AMS Networks

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.

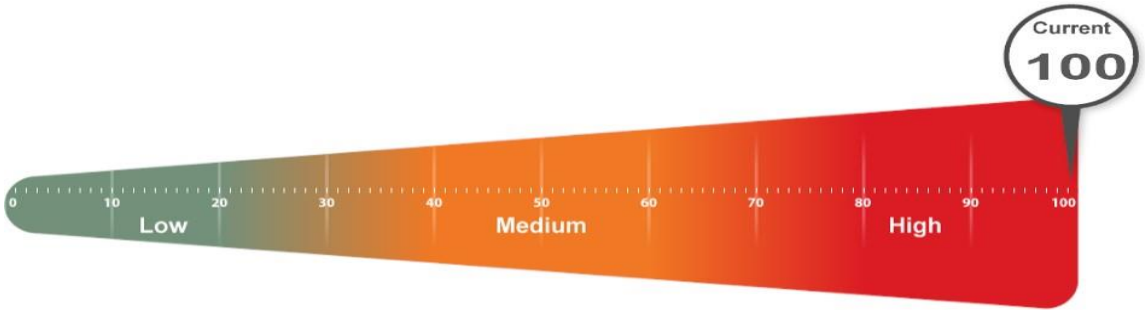
Risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their "risk score." The implementation components of the plan include:

- 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.

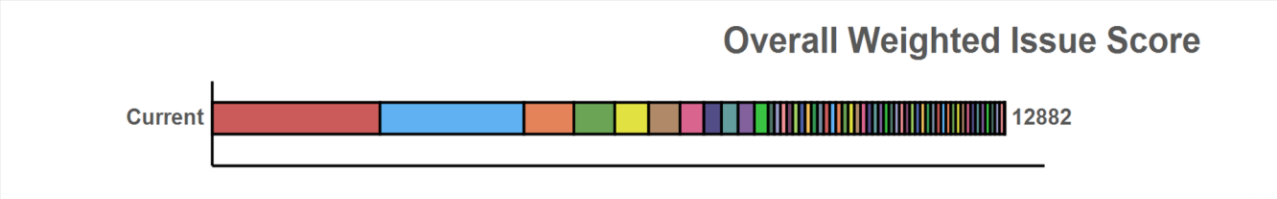


Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

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 (%)

	Automatic screen lock not turned on (94 pts each)
2726	***Current Score:*** 94 pts x 29 = 2726: 21.16%
	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.

	Remote Access Cloud Services could potentially expose ePHI either visually or through data transmission. (65 pts each)
2340	***Current Score:*** 65 pts x 36 = 2340: 18.16%
	Requirement: §164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
	Issue: Remote Access Cloud Services are in use and may pose potential ePHI risk.
	Recommendation: It is recommended to not use third-party remote access services on systems that could potentially display or access ePHI.

	Anti-spyware not up to date (90 pts each)
810	***Current Score:*** 90 pts x 9 = 810: 6.29%
	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.

	Significantly high number of Domain Administrators (35 pts each)
665	***Current Score:*** 35 pts x 19 = 665: 5.16%
	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 not logged in in 90 days (not terminated) (25 pts each)
550	***Current Score:*** 25 pts x 22 = 550: 4.27%
	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.

	User password set to never expire (30 pts each)
510	***Current Score:*** 30 pts x 17 = 510: 3.96%
	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.

	Unsupported operating systems (97 pts each)
388	***Current Score:*** 97 pts x 4 = 388: 3.01%
	Requirement: §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.
	Issue: 4 computers 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 on to domain in 30 days (13 pts each)
286	***Current Score:*** 13 pts x 22 = 286: 2.22%
	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-virus not up to date (90 pts each)
270	***Current Score:*** 90 pts x 3 = 270: 2.1%
	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.

	Computer with ePHI does not have object level auditing on (11 pts each)
264	***Current Score:*** 11 pts x 24 = 264: 2.05%
	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.

	Medium External Vulnerabilities Detected (75 pts each)
225	***Current Score:*** 75 pts x 3 = 225: 1.75%
	Requirement: §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure 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.

	Law Enforcement, Court Orders and Subpoenas - Training (100 pts each)

100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: §164.512(e) - Uses and Disclosure - Standard: Disclosures for judicial and administrative proceedings.
	Issue: Workforce members not trained in handling law enforcement requests, court orders, and subpoenas (not accompanied by a court order), and when to involve legal counsel.
	Recommendation: Ensure that everyone who may be involved with receiving and responding to law enforcement requests, court orders, and subpoenas (not accompanied by a court order) has been trained and reminded what procedures are to be followed.

	No Minimum Necessary Access Training (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: §164.502(e) Uses and disclosures of protected health information, §164.504(e) - Uses and disclosures - organizational requirements, §164.532(d) - Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.
	Issue: Workforce members not trained in HIPAA's requirements for Minimum Necessary Access.
	Recommendation: Ensure that all workforce members have been trained and reminded what procedures are to be followed.

	No written Patient's Right to Access Records Policy (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: § 164.520 - Notice of Privacy Practices for protected health information.
	Issue: No written Policy and Procedures that include the rights of a patient to access their records.
	Recommendation: Create a written policy requiring compliance with all state and federal requirements related to patients accessing their medical records.

	No Confidential Communications Policy (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: § 164.522(b) - Rights to request privacy protection for protected health information - Confidential communications requirements.
	Issue: No Policies and Procedures include the HIPAA's requirements for confidential communications.
	Recommendation: Implement a written policy to ensure compliance with HIPAA's requirements for confidential communications.

	Notice of Privacy Practices Not Prominently Displayed on Website (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: § 164.520 - Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.
	Issue: Notice of Privacy Practices not prominently displayed on your website as required by HIPAA.

Recommendation: Ensure that a link to a downloadable Notice of Privacy Practices be displayed prominently on your website.

	No Training on Business Associates (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: § 164.502(e) Uses and disclosures of protected health information, § 164.504(e) - Uses and disclosures - organizational requirements, § 164.532(d) - Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.
	Issue: Workforce members not trained in managing Business Associate relationships.
	Recommendation: Ensure that everyone who may be involved with Business Associates have been trained and reminded what procedures are to be followed.

	Authorizations for Uses & Disclosures (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: §164.508 - Uses and disclosures requiring an opportunity for the individual to agree or to object - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.
	Issue: No Policies and Procedures include the requirements for authorizations for use and disclosures.
	Recommendation: Implement a written policy to ensure compliance with HIPAA's requirements for Authorizations for Uses & Disclosures.

	Missing Notice of Privacy Practices Policy (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: § 164.520 - Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.
	Issue: No Written Notice of Privacy Practices Policy.
	Recommendation: Create an organizational policy requiring that a Notice of Privacy Practices be written to comply with requirements of the HIPAA and HITECH Acts, and be given to all new patients who acknowledge receipt in writing; prominently displayed in patient areas; available to all who request it; and prominently displayed on your website.

	No training on Uses & Disclosures - Emergencies & Disasters (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: §164.510(b) - Uses and disclosures for which authorization is required - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.
	Issue: Workforce members not trained disclosures during emergencies and disasters.
	Recommendation: Ensure that all workforce members have been trained and reminded what procedures are to be followed during emergencies and disasters.

	Breach Complaint and Determination Training (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: §164.530(b) - Administrative requirements - Standard: Training and Implementation specifications: Training.
	Issue: Breach Complaint and Determination Training
	Recommendation: Ensure that all workforce members receive training pertaining to the Breach Notification Rule.

	Business Associate won't sign agreement for Data Center that could expose ePHI (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	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: Business Associate agreements should be signed by Data Centers that host servers containing ePHI or connect to computers that contain ePHI.
	Recommendation: Acquire Business Associate agreements with Data Centers in use by the company.

	Breach Risk Assessment Training (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: §164.530(b) - Administrative requirements - Standard: Training and Implementation specifications: Training.
	Issue: No Breach Risk Assessment Training.
	Recommendation: Ensure that all applicable workforce members receive training pertaining to the Breach Notification Rule's requirements for a risk assessment.

	Business Associate won't sign agreement for Cloud Service that could expose ePHI (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	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: Cloud Services may advertently or inadvertently be used to transmit ePHI and should sign Business Associate agreements.
	Recommendation: Acquire Business Associate agreements with Cloud Services in use by the company.

	Breach Individual Notification Training (100 pts each)

100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: §164.530(b) - Administrative requirements - Standard: Training and Implementation specifications: Training.
	Issue: No Breach Individual Notification Training.
	Recommendation: Ensure that all applicable workforce members receive training pertaining to the Breach Notification Rule's requirements for notifying individuals after a breach.

	No HIPAA-related Marketing Policy Training (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: §164.501 - Definitions: Marketing, §164.508(a)(3) - Authorizations for uses and disclosures - Authorization: Marketing.
	Issue: Appropriate workforce members not trained in HIPAA's requirements related to marketing
	Recommendation: Ensure that everyone who may be involved with marketing has been trained and reminded what procedures are to be followed.

	Breach Reporting Training (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 0.78%
	Requirement: §164.530(b) - Administrative requirements - Standard: Training and Implementation specifications: Training.
	Issue: Breach Reporting Training.
	Recommendation: Ensure that all workforce members receive training pertaining to the Breach Notification Rule.

	Anti-spyware not installed (94 pts each)
94	***Current Score:*** 94 pts x 1 = 94: 0.73%
	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)
94	***Current Score:*** 94 pts x 1 = 94: 0.73%
	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.

	Firewall does not support IPS (88 pts each)
88	***Current Score:*** 88 pts x 1 = 88: 0.68%
	Requirement: §164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
	Issue: Firewalls without an Intrusion Prevention System (IPS) may not adequately protect the environment against malicious external attacks.
	Recommendation: Enable IPS on firewalls or investigate putting in place a firewall with IPS capabilities.

	Missing written ePHI Transmission Encryption Procedure (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%
	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 Data Integrity Protection Procedure (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%
	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 Media Reuse Policy (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%
	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 Data Backup and Storage Procedure (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%

	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 evidence of ongoing monitoring and planning to evaluate security plans and procedures (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%
	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 Emergency Mode Operations Plan (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%
	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 Security Incident Response and Reporting Plan (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%
	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 Sanction Policy (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%
	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 Facility Security Plan (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%
	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 written Workstation Security Procedure (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.66%
	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 procedure for maintaining Facility Access Control maintenance records (82 pts each)
82	***Current Score:*** 82 pts x 1 = 82: 0.64%
	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.

	Missing Evidence - Business Associates Policy (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: § 164.502(e) Uses and disclosures of protected health information, § 164.504(e) - Uses and disclosures - organizational requirements, § 164.532(d) - Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.
	Issue: Copy Business Associates Policy not attached.
	Recommendation: Attach copy of Business Associates Policy.

	Missing Evidence - Notice of Privacy Practices (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: §164.520 - Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.
	Issue: Copy of Notice of Privacy Practices not attached.
	Recommendation: Attach a copy of the Notice of Privacy Practices

	Missing Evidence - Uses & Disclosures - Emergencies & Disasters (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: §164.510(b) - Uses and disclosures for which authorization is required - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.
	Issue: Copy Uses & Disclosures - Emergencies & Disasters not attached.
	Recommendation: Attach copy Uses & Disclosures - Emergencies & Disasters.

	Missing Evidence - Breach Reporting Policy (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: §164.408 - Notification to the Secretary - Standard: A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2) notify the Secretary of HHS.
	Issue: No documents related to Breach Reporting Policy attached.
	Recommendation: Attach a copy of the Policy & Procedures Document or portion related to the Breach Reporting Policy.

	Missing Evidence - Law Enforcement, Court Orders and Subpoenas Policy (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: §164.512(e) - Uses and Disclosure - Standard: Disclosures for judicial and administrative proceedings.
	Issue: Copy of Law Enforcement, Court Orders and Subpoenas Policy not attached.
	Recommendation: Attach copy of Law Enforcement, Court Orders and Subpoenas Policy.

	Missing Evidence - Minimum Necessary Access Policy. (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: §164.502(e) Uses and disclosures of protected health information, §164.504(e) - Uses and disclosures - organizational requirements, §164.532(d) - Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.
	Issue: Copy of Minimum Necessary Access Policy not attached.
	Recommendation: Attach copy of Minimum Necessary Access Policy.

	Missing Evidence - Minimum Necessary Access Internal Auditing (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: §164.502(e) Uses and disclosures of protected health information, §164.504(e) - Uses and disclosures - organizational requirements, §164.532(d) - Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.
	Issue: Records of reviews of access to paper and electronic records not attached.
	Recommendation: Attach evidence of minimum necessary access internal auditing including, records of reviews of access to paper and electronic records.

	Missing Evidence - HIPAA-related Marketing Policy (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: §164.501 - Definitions: Marketing, §164.508(a)(3) - Authorizations for uses and disclosures - Authorization: Marketing.
	Issue: Copy of HIPAA-related Marketing Policy not attached.
	Recommendation: Attach copy of HIPAA-related Marketing Policy.

	Missing Evidence - Breach Individual Notification Policy (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: §164.404 - Notification to individuals - Standard: General rule for unsecured protected health information breach notification.
	Issue: No documents related to Breach Individual Notification Policy attached.
	Recommendation: Attach a copy of the Policy & Procedures Document or portion related to the Breach Individual Notification Policy.

	Missing Evidence - Breach Risk Assessment Policy (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.62%
	Requirement: §164.402 - Definitions - Risk assessment of breach.
	Issue: No documents related to Breach Risk Assessment Policy attached.
	Recommendation: Attach a copy of the Policy & Procedures Document or portion related to the Breach Risk Assessment Policy.

	Account lockout disabled (77 pts each)
77	***Current Score:*** 77 pts x 1 = 77: 0.6%
	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.

	Few Security patches missing on computers with ePHI (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 0.58%
	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. Few is defined as missing 3 or less patches.
	Recommendation: Address patching on computers missing 1-3 security patches.

	Passwords less than 8 characters allowed (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 0.58%
	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.

	Firewall malware filtering subscription not up-to-date (12 pts each)
12	***Current Score:*** 12 pts x 1 = 12: 0.09%
	Requirement: §164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.
	Issue: Out-of-date malware filtering subscriptions may not protect the network against malicious software.
	Recommendation: Ensure malware filtering subscriptions are up-to-date.

	Use of generic logins (1 pts each)
1	***Current Score:*** 1 pts x 1 = 1: 0.01%
	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.