NNT HIPAA Microsoft Member Server 2016 Benchmark
17/10/2018 16:04
2016-GENVII-MPK (169.254.164.52,192.168.17.237)

Compliance Score : 49.57%

287 of 580 rules passed
1 of 580 rules partially passed
292 of 580 rules failed

4.1. Security Management Process (§ 164.308(a)(1))
1. HIPAA Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.
Identify Relevant Information Systems (Network Inventory Scan), Conduct Risk Assessment (Assess Configuration Vulnerabilities), Implement a Risk Management Program (Assess Software Vulnerabilities).

Rule Name	Result
Identify all information systems that house EPHI, including all hardware	Pass: This rule is not automatically assessed. Verify that Inventory Scan results, Secure Build assessments and Vulnerability Scans are regularly reviewed.

4.2 Assigned Security Responsibility (§ 164.308(a)(2))
HIPAA Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity
Identify the individual who has final responsibility for security, document the assignment to one individual's responsibilities in a job description

Rule Name	Result
Who in the organization is authorized to accept risk from information	Pass: This rule is not automatically assessed. You must Identify the individual who has final responsibility for security, document the assignment to one

4.3 Workforce Security (§ 164.308(a)(3))
HIPAA Standard: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information
1 - 3. Implement Procedures for Authorization and/or Supervision, Establish Clear Job Descriptions and Responsibilities, Establish Criteria and Procedures for Hiring, Workforce Clearance and Termination

Rule Name	Result
Implement Procedures for Authorization and/or Supervision	Pass: This rule is not automatically assessed. You must implement policies and procedures to ensure that all members of its workforce have appropriate

4.4 Information Access Management (§ 164.308(a)(4))
HIPAA Standard: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements
Isolate Healthcare Clearinghouse Functions, Implement Policies and Procedures for Authorizing Access, Implement Policies and Procedures for Access Establishment and Modification

Rule Name	Result
Determine if a component of the covered entity constitutes a healthcare	Pass: This rule is not automatically assessed. You must implement policies and procedures for authorizing access to electronic protected health information

4.5 Security Awareness and Training (§ 164.308(a)(5))
HIPAA Standard: Implement a security awareness and training program for all members of its workforce (including management)
Conduct a Training Needs Assessment, Develop and Approve a Training Strategy and a Plan, Develop Appropriate Awareness and Training Content, Materials, and Methods

Rule Name	Result
Implement a security awareness and training program for all members	Pass: This rule is not automatically assessed. You must implement a security awareness and training program for all members of its workforce (including

4.6. Security Incident Procedures (§ 164.308(a)(6)))
HIPAA Standard: Implement policies and procedures to address security incidents.
Determine Goals of Incident Response, Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism, Develop and Implement Procedures to Respond to and Report Security

Rule Name	Result
Implement policies and procedures to address security incidents.	Pass: This rule is not automatically assessed. Implement policies and procedures to address security incidents.

4.7. Contingency Plan (§ 164.308(a)(7))

HIPAA Standard: 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

Develop Contingency Planning Policy, conduct an Applications and Data Criticality Analysis, Identify Preventive Measures

Rule Name	Result
Establish policies and procedures for responding to an emergency or	Pass: This rule is not automatically assessed. Establish policies and procedures for responding to an emergency or other occurrence.

4.8. Evaluation (§ 164.308(a)(8))

HIPAA Standard: 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

Determine Whether Internal or External Evaluation Is Most Appropriate, Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule, Conduct, Document and Repeat

Rule Name	Result
Perform a periodic technical and nontechnical evaluation.	Pass: This rule is not automatically assessed. Perform a periodic technical and nontechnical evaluation.

4.9. Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))

HIPAA Standard: A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered

Identify Entities that Are Business Associates under the HIPAA Security Rule, Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met, Implement An

Rule Name	Result
The covered entity must obtain, document and measure performance of	Pass: This rule is not automatically assessed. The covered entity must obtain, document and measure performance of satisfactory assurances that the

4.10. Facility Access Controls (§ 164.310(a)(1))

HIPAA Standard: 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.

Conduct an Analysis of Existing Physical Security Vulnerabilities and Identify Corrective Measures. Develop a Facility Security Plan, Access Control and Validation Procedures, Contingency Operations Procedures and Maintain

Rule Name	Result
Inventory facilities and identify shortfalls and/or vulnerabilities in current	Pass: This rule is not automatically assessed. Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities, correct

4.11. Workstation Use (§ 164.310(b))

HIPAA Standard: General System Hardening - 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

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: System Hardening - Default User Accounts

Rule Name	Result
Ensure 'Accounts: Guest account status' is set to 'Disabled'	Pass: PASSED:.
Configure 'Accounts: Rename administrator account'	Fail: FAILED: (L1) Configure 'Accounts: Rename administrator account' : securitypolicy (2 items: "Administrator", "Administrator"). Remediation : To establish
Configure 'Accounts: Rename guest account'	Fail: FAILED: (L1) Configure 'Accounts: Rename guest account' : securitypolicy (2 items: "Guest", "Guest"). Remediation : To establish the recommended
Ensure 'Enable screen saver' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Enable screen saver' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the following
Ensure 'Force specific screen saver: Screen saver executable name' is	Fail: FAILED: (L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' : .". Remediation : To establish the
Ensure 'Password protect the screen saver' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set
Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer,	The rule requires that All tests pass. Fail: FAILED: (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' : .". Remediation :
Ensure 'Turn off Help Experience Improvement Program' is set to	Fail: FAILED: (L2) Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' : .". Remediation : To establish the recommended
Ensure 'Allow Use of Camera' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Allow Use of Camera' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set the following

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: System Hardening - Attachment Manager Rules

Rule Name	Result
Ensure 'Do not preserve zone information in file attachments' is set to	Fail: FAILED: (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' : .". Remediation : To establish the recommended

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: System Hardening: Group Policy Rules

Rule Name	Result
Ensure 'Configure registry policy processing: Do not apply during	Fail: FAILED: (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' : .".
Ensure 'Configure registry policy processing: Process even if the Group	Fail: FAILED: (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' : .".
Ensure 'Continue experiences on this device' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Continue experiences on this device' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP,
Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'	Pass: PASSED: 1".

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Internet Communication settings Rules

Rule Name	Result
Ensure 'Turn off access to the Store' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Turn off access to the Store' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the
Ensure 'Turn off downloading of print drivers over HTTP' is set to	Fail: FAILED: (L2) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' : .". Remediation : To establish the recommended
Ensure 'Turn off handwriting personalization data sharing' is set to	Fail: FAILED: (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' : .". Remediation : To establish the recommended

Ensure 'Turn off handwriting recognition error reporting' is set to	Fail: FAILED: (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' : .". Remediation : To establish the recommended configuration
Ensure 'Turn off Internet Connection Wizard if URL connection is	Fail: FAILED: (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' : .". Remediation : To
Ensure 'Turn off Internet download for Web publishing and online	Fail: FAILED: (L2) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' : .". Remediation : To establish the
Ensure 'Turn off printing over HTTP' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the
Ensure 'Turn off Registration if URL connection is referring to	Fail: FAILED: (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' : .". Remediation : To establish the
Ensure 'Turn off Search Companion content file updates' is set to	Fail: FAILED: (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' : .". Remediation : To establish the recommended
Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP,
Ensure 'Turn off the "Publish to Web" task for files and folders' is set to	Fail: FAILED: (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' : .". Remediation : To establish the recommended
Ensure 'Turn off the Windows Messenger Customer Experience	Fail: FAILED: (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' : .". Remediation : To establish
Ensure 'Turn off Windows Customer Experience Improvement Program'	Fail: FAILED: (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' : .". Remediation : To establish the
Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Personalization Rules

Rule Name	Result
Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (CCE	Fail: FAILED: (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP,
Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via
Ensure 'Allow Input Personalization' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Allow Input Personalization' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set the

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Search Rules

Rule Name	Result
Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set
Ensure 'Allow Cortana' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Allow Cortana' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set the following UI
Ensure 'Allow Cortana above lock screen' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set
Ensure 'Allow search and Cortana to use location' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Windows Installer Rules

Rule Name	Result
Ensure 'Allow user control over installs' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Allow user control over installs' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set the
Ensure 'Always install with elevated privileges' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP,
Ensure 'Prevent Internet Explorer security prompt for Windows Installer	Fail: FAILED: (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' : .". Remediation : To establish the
Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via
Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set
Ensure 'Allow Remote Shell Access' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled' : .". Remediation : To implement the recommended configuration state, set the
Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' : .". Remediation : To establish the recommended configuration
Ensure 'Prevent users from sharing files within their profile.' is set to	Fail: FAILED: (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' : .". Remediation : To establish the recommended
Ensure 'Always install with elevated privileges' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP,
Ensure 'Prevent Codec Download' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Prevent Codec Download' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Administrative Templates (Computer) Rules	
Rule Name	**Result**
Ensure 'Apply UAC restrictions to local accounts on network logons' is	Fail: FAILED: (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) : .". Remediation : To establish the
Ensure 'WDigest Authentication' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'WDigest Authentication' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set the
Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only)	Fail: FAILED: (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) : .". Remediation : In order to utilize LAPS, a minor Active Directory
Ensure 'Do not allow password expiration time longer than required by	Fail: FAILED: (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) : .". Remediation : To establish
Ensure 'Enable Local Admin Password Management' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) : .". Remediation : To establish the recommended
Ensure 'Password Settings: Password Complexity' is set to 'Enabled:	Fail: FAILED: (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS
Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or	Fail: FAILED: (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) : .'0'. Remediation : To establish the
Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30	Fail: FAILED: (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) : .'31'. Remediation : To establish the
Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual	Fail: FAILED: (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and
Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set	Fail: FAILED: (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') : .". Remediation : To establish the recommended
Ensure 'Configuration of wireless settings using Windows Connect Now'	The rule requires that All tests pass. Fail: FAILED: (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' : .".
Ensure 'Prohibit access of the Windows Connect Now wizards' is set to	Fail: FAILED: (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' : .". Remediation : To establish the recommended
Ensure 'Minimize the number of simultaneous connections to the	Fail: FAILED: (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' : .". Remediation : To
Ensure 'Prohibit connection to non-domain networks when connected to	Fail: FAILED: (L2) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) : .".
Ensure 'Include command line in process creation events' is set to	Fail: FAILED: (L1) Ensure 'Include command line in process creation events' is set to 'Disabled' : .". Remediation : To establish the recommended
Ensure 'Disallow copying of user input methods to the system account	Fail: FAILED: (L2) Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' : .". Remediation : To establish the
Ensure 'Block user from showing account details on sign-in' is set to	Fail: FAILED: (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' : .". Remediation : To implement the recommended
Ensure 'Untrusted Font Blocking' is set to 'Enabled: Block untrusted	Fail: FAILED: (L1) Ensure 'Untrusted Font Blocking' is set to 'Enabled: Block untrusted fonts and log events' : .". Remediation : To establish the
Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' : .". Remediation : To establish the recommended configuration
Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set
Ensure 'Allow network connectivity during connected-standby (on	Fail: FAILED: (L2) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' : .". Remediation : To establish the
Ensure 'Allow network connectivity during connected-standby (plugged	Fail: FAILED: (L2) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' : .". Remediation : To establish the
Ensure 'Require a password when a computer wakes (on battery)' is set	Fail: FAILED: (L2) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' : .". Remediation : To establish the recommended
Ensure 'Require a password when a computer wakes (plugged in)' is	Fail: FAILED: (L2) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' : .". Remediation : To establish the recommended
Ensure 'Turn off the advertising ID' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Turn off the advertising ID' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the
Ensure 'Enable Windows NTP Client' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the
Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only)	Fail: FAILED: (L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) : .". Remediation : To establish the recommended configuration via
Ensure 'Allow a Windows app to share application data between users'	Fail: FAILED: (L2) Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' : .". Remediation : To establish the
Ensure 'Let Windows apps *' is set to 'Enabled: Force Deny'	Fail: FAILED: (L2) Ensure 'Let Windows apps *' is set to 'Enabled: Force Deny' : .". Remediation : To establish the recommended configuration via GP, set
Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via
Ensure 'Require pin for pairing' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Require pin for pairing' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the following
Ensure 'Do not display the password reveal button' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via
Ensure 'Enumerate administrator accounts on elevation' is set to	Fail: FAILED: (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' : .". Remediation : To establish the recommended
Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise	Fail: FAILED: (L1) Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]' : .". Remediation : To establish the recommended configuration
Ensure 'Disable pre-release features or settings' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Disable pre-release features or settings' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via
Ensure 'Do not show feedback notifications' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set
Ensure 'Toggle user control over Insider builds' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP,
Ensure 'Configure Windows SmartScreen' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Configure Windows SmartScreen' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set
Ensure 'Turn off Data Execution Prevention for Explorer' is set to	Fail: FAILED: (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' : .". Remediation : To establish the recommended
Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via
Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP,
Ensure 'Turn off location' is set to 'Enabled' (CCE Reference : CCE-	Fail: FAILED: (L2) Ensure 'Turn off location' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the following UI
Ensure 'Allow Extensions' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Allow Extensions' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set the following UI
Ensure 'Allow InPrivate Browsing' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Allow InPrivate Browsing' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set the
Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party	Fail: FAILED: (L1) Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party cookies' or higher : .'2'. Remediation : To establish the recommended
Ensure 'Configure Password Manager' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Configure Password Manager' is set to 'Disabled' : .". Remediation : To establish the recommended configuration via GP, set the

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Administrative Templates (Computer) Rules	
Rule Name	**Result**
Ensure 'Configure Pop-up Blocker' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Configure Pop-up Blocker' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the
Ensure 'Configure search suggestions in Address bar' is set to	Fail: FAILED: (L1) Ensure 'Configure search suggestions in Address bar' is set to 'Disabled' : .". Remediation : To establish the recommended configuration
Ensure 'Configure SmartScreen Filter' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Configure SmartScreen Filter' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the

Ensure 'Prevent access to the about:flags page in Microsoft Edge' is set	Fail: FAILED: (L2) Ensure 'Prevent access to the about:flags page in Microsoft Edge' is set to 'Enabled' : .''. Remediation : To establish the recommended
Ensure 'Prevent bypassing SmartScreen prompts for files' is set to	Fail: FAILED: (L2) Ensure 'Prevent bypassing SmartScreen prompts for files' is set to 'Enabled' : .''. Remediation : To establish the recommended
Ensure 'Prevent bypassing SmartScreen prompts for sites' is set to	Fail: FAILED: (L2) Ensure 'Prevent bypassing SmartScreen prompts for sites' is set to 'Enabled' : .''. Remediation : To establish the recommended
Ensure 'Prevent using Localhost IP address for WebRTC' is set to	Fail: FAILED: (L2) Ensure 'Prevent using Localhost IP address for WebRTC' is set to 'Enabled' : .''. Remediation : To establish the recommended
Ensure 'Prevent the usage of OneDrive for file storage' is set to	Fail: FAILED: (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' : .''. Remediation : To establish the recommended configuration
Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' : .''. Remediation : To establish the recommended configuration via
Ensure 'Disable all apps from Windows Store' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Disable all apps from Windows Store' is set to 'Enabled' : .''. Remediation : To establish the recommended configuration via GP,
Ensure 'Turn off Automatic Download and Install of updates' is set to	Fail: FAILED: (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' : .''. Remediation : To establish the recommended
Ensure 'Turn off the offer to update to the latest version of Windows' is	Fail: FAILED: (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' : .''. Remediation : To establish the recommended
Ensure 'Turn off the Store application' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Turn off the Store application' is set to 'Enabled' : .''. Remediation : To establish the recommended configuration via GP, set the
Ensure 'Join Microsoft MAPS' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' : False.''. Remediation : To establish the recommended configuration via GP, set the
Ensure 'Configure Watson events' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Configure Watson events' is set to 'Disabled' : .''. Remediation : To establish the recommended configuration via GP, set the
Ensure 'Allow suggested apps in Windows Ink Workspace' is set to	Fail: FAILED: (L2) Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' : .''. Remediation : To establish the recommended
Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but	Fail: FAILED: (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On' :
Ensure 'Configure Windows spotlight on Lock Screen' is set to	Fail: FAILED: (L2) Ensure 'Configure Windows spotlight on Lock Screen' is set to Disabled' : .''. Remediation : To establish the recommended configuration
Ensure 'Do not suggest third-party content in Windows spotlight' is set	Fail: FAILED: (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' : .''. Remediation : To establish the recommended
Ensure 'Turn off all Windows spotlight features' is set to 'Enabled'	Fail: FAILED: (L2) Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' : .''. Remediation : To establish the recommended configuration via GP,

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: App runtime Rules

Rule Name	Result
Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' : .''. Remediation : To establish the recommended configuration via GP,
Ensure 'Block launching Windows Store apps with Windows Runtime	Fail: FAILED: (L2) Ensure 'Block launching Windows Store apps with Windows Runtime API access from hosted content.' is set to 'Enabled' : .''.

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: User Account Control Rules

Rule Name	Result
Ensure 'User Account Control: Admin Approval Mode for the Built-in	Fail: FAILED: (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' : .'0'. Remediation : To
Ensure 'User Account Control: Allow UIAccess applications to prompt	Pass: PASSED: '0'.
Ensure 'User Account Control: Behavior of the elevation prompt for	Fail: FAILED: (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent
Ensure 'User Account Control: Behavior of the elevation prompt for	Fail: FAILED: (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' : .'3'.
Ensure 'User Account Control: Detect application installations and	Pass: PASSED: '1'.
Ensure 'User Account Control: Only elevate UIAccess applications that	Pass: PASSED: '1'.
Ensure 'User Account Control: Run all administrators in Admin Approval	Pass: PASSED: '1'.
Ensure 'User Account Control: Switch to the secure desktop when	Pass: PASSED: '1'.
Ensure 'User Account Control: Virtualize file and registry write failures to	Pass: PASSED: '1'.

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: AutoPlay Policies Rules

Rule Name	Result
Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' : .''. Remediation : To establish the recommended configuration via
Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not	Fail: FAILED: (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' : .''. Remediation : To establish
Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	Fail: FAILED: (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' : .''. Remediation : To establish the recommended configuration via GP, set the

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: EMET Rules

Rule Name	Result
Ensure EMET is installed	Fail: Ensure EMET is installed : .". Remediation : Install EMET 5 or higher.
Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'	Fail: (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' : .'0'. Remediation : To establish the recommended configuration via GP, set the
Ensure 'Default Protections for Popular Software' is set to 'Enabled'	Fail: (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled' : .'0'. Remediation : To establish the recommended configuration via GP, set
Ensure 'Default Protections for Recommended Software' is set to	Fail: (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled' : .'0'. Remediation : To establish the recommended configuration via
Set 'System ASLR' to 'Enabled:Application Opt-In'	Fail: Set 'System ASLR' to 'Enabled:Application Opt-In' : .". Remediation : To establish the recommended configuration via GP, set the following UI path to
Set 'System DEP' to 'Enabled:Application Opt-Out'	Fail: Set 'System DEP' to 'Enabled:Application Opt-Out' : .". Remediation : To establish the recommended configuration via GP, set the following UI path to
Set 'System SEHOP' to 'Enabled:Application Opt-Out'	Fail: Set 'System SEHOP' to 'Enabled:Application Opt-Out' : .". Remediation : To establish the recommended configuration via GP, set the following UI path

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Account Policies - User Rights Assignment

Rule Name	Result
Ensure 'Access Credential Manager as a trusted caller' is set to 'No	Pass: PASSED: securitypolicy ().
Configure 'Access this computer from the network'	Fail: FAILED: (L1) Configure 'Access this computer from the network' : securitypolicy (3 items: EVERYONE, BUILTIN\USERS, BUILTIN\BACKUP
Ensure 'Act as part of the operating system' is set to 'No One'	Pass: PASSED:.
Ensure 'Adjust memory quotas for a process' is set to 'Administrators,	Fail: FAILED: (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' : securitypolicy (6 items:
Configure 'Allow log on locally'	Fail: FAILED: (L1) Configure 'Allow log on locally' : securitypolicy (2 items: BUILTIN\USERS, BUILTIN\BACKUP OPERATORS). Remediation : To establish
Configure 'Allow log on through Remote Desktop Services'	Pass: PASSED: securitypolicy (2 items: BUILTIN\ADMINISTRATORS, BUILTIN\REMOTE DESKTOP USERS).
Ensure 'Back up files and directories' is set to 'Administrators'	Fail: FAILED: (L1) Ensure 'Back up files and directories' is set to 'Administrators' : securitypolicy (BUILTIN\BACKUP OPERATORS). Remediation : To
Ensure 'Change the system time' is set to 'Administrators, LOCAL	Pass: PASSED: securitypolicy (2 items: NT AUTHORITY\LOCAL SERVICE, BUILTIN\ADMINISTRATORS).
Ensure 'Change the time zone' is set to 'Administrators, LOCAL	Pass: PASSED: securitypolicy (2 items: NT AUTHORITY\LOCAL SERVICE, BUILTIN\ADMINISTRATORS).
Ensure 'Create a pagefile' is set to 'Administrators'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Ensure 'Create a token object' is set to 'No One'	Pass: PASSED: securitypolicy ().
Ensure 'Create global objects' is set to 'Administrators, LOCAL	Pass: PASSED: securitypolicy (4 items: NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE, BUILTIN\ADMINISTRATORS, NT
Ensure 'Create permanent shared objects' is set to 'No One'	Pass: PASSED: securitypolicy ().
Configure 'Create symbolic links'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Ensure 'Debug programs' is set to 'Administrators'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Configure 'Enable computer and user accounts to be trusted for	Pass: PASSED: securitypolicy ().
Ensure 'Force shutdown from a remote system' is set to 'Administrators'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Configure 'Impersonate a client after authentication'	Fail: FAILED: (L1) Configure 'Impersonate a client after authentication' : securitypolicy (BUILTIN\IIS_IUSRS). Remediation : To establish the recommended
Ensure 'Increase scheduling priority' is set to 'Administrators'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Ensure 'Load and unload device drivers' is set to 'Administrators'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Ensure 'Lock pages in memory' is set to 'No One'	Pass: PASSED: securitypolicy ().
Ensure 'Modify an object label' is set to 'No One'	Pass: PASSED: securitypolicy ().
Ensure 'Modify firmware environment values' is set to 'Administrators'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Ensure 'Profile single process' is set to 'Administrators'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Ensure 'Profile system performance' is set to 'Administrators, NT	Pass: PASSED: securitypolicy (2 items: BUILTIN\ADMINISTRATORS, NT SERVICE\WDISERVICEHOST).
Ensure 'Replace a process level token' is set to 'LOCAL SERVICE,	Fail: FAILED: (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' : securitypolicy (6 items:
Ensure 'Restore files and directories' is set to 'Administrators'	Fail: FAILED: (L1) Ensure 'Restore files and directories' is set to 'Administrators' : securitypolicy (BUILTIN\BACKUP OPERATORS). Remediation : To
Ensure 'Shut down the system' is set to 'Administrators'	Fail: FAILED: (L1) Ensure 'Shut down the system' is set to 'Administrators' : securitypolicy (BUILTIN\BACKUP OPERATORS). Remediation : To establish the
Ensure 'Take ownership of files or other objects' is set to	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Windows Update Rules

Rule Name	Result
Ensure 'Configure Automatic Updates' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' : .". Remediation : To establish the recommended configuration via GP, set the
Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0	Fail: FAILED: (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' : .". Remediation : To establish the recommended
Set 'Do not adjust default option to 'Install Updates and Shut Down' in	Fail: Set 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' to 'Disabled' : .". Remediation : To establish the
Set 'Do not display 'Install Updates and Shut Down' option in Shut	Fail: Set 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' to 'Disabled' : .". Remediation : To establish the
Ensure 'No auto-restart with logged on users for scheduled automatic	Fail: FAILED: (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' : .". Remediation : To
Set 'Reschedule Automatic Updates scheduled installations' to	Fail: Set 'Reschedule Automatic Updates scheduled installations' to 'Enabled:1 minute' : ." ". Remediation : To establish the recommended configuration via
Ensure 'Select when Feature Updates are received' is set to 'Enabled:	The rule requires that All tests pass. Fail: FAILED: (L1) Ensure 'Select when Feature Updates are received' is set to 'Enabled: Current Branch for Business,
Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0	The rule requires that All tests pass. Fail: FAILED: (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' : .". Remediation : To

HIPAA Standard: Non-Default Services List - 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

Non-Default Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any Non-Default Services

Rule Name	Result
Check for any Non-Default Services	Fail: Services installed not covered by Default and Optional services list: WpnUserService_11c6fe (wpnuserservice_11c6fe), UserDataSvc_11c6fe

Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mandatory Services

Rule Name	Result
AllJoyn Router Service (Hardened Start Mode: Manual, Hardened	
App Readiness Service (Hardened Start Mode: Manual, Hardened	
Application Host Helper Service (Hardened Start Mode: Auto, Hardened	
Application Identity Service (Hardened Start Mode: Manual, Hardened	
Application Information Service (Hardened Start Mode: Manual,	
Application Layer Gateway Service (Hardened Start Mode: Disabled,	
Application Management Service (Hardened Start Mode: Manual,	
AppX Deployment Service (AppXSVC) Service (Hardened Start Mode:	
ASP.NET State Service (aspnet_state) Service (Hardened Start Mode:	
ActiveX Installer (AxInstSV) Service (Hardened Start Mode: Disabled,	
Auto Time Zone Updater (tzautoupdate) Service (Hardened Start Mode:	
Background Intelligent Transfer Service (Hardened Start Mode: Manual,	
Background Tasks Infrastructure (BrokerInfrastructure) Service	
Base Filtering Engine Service (Hardened Start Mode: Auto, Hardened	
Bluetooth Support Service (bthserv) Service (Hardened Start Mode:	
CDPUserSvc (cdpusersvc) Service (Hardened Start Mode: Disabled,	
Certificate Propagation Service (Hardened Start Mode: Manual,	
Client License Service (ClipSVC) Service (Hardened Start Mode:	
CNG Key Isolation Service (Hardened Start Mode: Manual, Hardened	
COM+ Event System Service (Hardened Start Mode: Auto, Hardened	
COM+ System Application Service (Hardened Start Mode: Manual,	
Computer Browser Service (Hardened Start Mode: Disabled, Hardened	
Connected Devices Platform Service (CDPSvc) Service (Hardened	
Connected User Experiences and Telemetry (DiagTrack) Service	
Contact Data (PimIndexMaintenanceSvc) Service (Hardened Start	
CoreMessaging (CoreMessagingRegistrar) Service (Hardened Start	
Credential Manager Service (Hardened Start Mode: Manual, Hardened	
Cryptographic Services Service (Hardened Start Mode: Auto, Hardened	
Data Sharing (DsSvc) Service (Hardened Start Mode: Manual,	
Data Sharing (DcpSvc) Service (Hardened Start Mode: Manual,	

Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mandatory Services

Rule Name	Result
DCOM Server Process Launcher Service (Hardened Start Mode: Auto,	
Device Association (deviceassociationservice) Service (Hardened Start	
Device Install (DeviceInstall) Service (Hardened Start Mode: Manual,	

Device Management Enrollment (DmEnrollmentSvc) Service (Hardened	
Device Setup (DsmSvc) Service (Hardened Start Mode: Manual,	
DevQuery Background Discovery Broker (DevQueryBroker) Service	
DHCP Client Service (Hardened Start Mode: Auto, Hardened Expected	
Diagnostic Policy Service (Hardened Start Mode: Auto, Hardened	
Diagnostic Service Host Service (Hardened Start Mode: Disabled,	Fail: state WdiServiceHost (running), startmode WdiServiceHost (manual).
Diagnostic System Host Service (Hardened Start Mode: Disabled,	Fail: state WdiSystemHost (stopped), startmode WdiSystemHost (manual).
Distributed Link Tracking Client Service (Hardened Start Mode: Auto,	
Distributed Transaction Coordinator Service (Hardened Start Mode:	
DMWAPPushService (dmwappushservice) Service (Hardened Start	
DNS Client Service (Hardened Start Mode: Auto, Hardened Expected	
Downloaded Maps Manager (MapsBroker) Service (Hardened Start	
Embedded Mode (embeddedmode) Service (Hardened Start Mode:	
The Enhanced Mitigation Experience Toolkit (EMET) Service	
Encrypting File System (EFS) Service (Hardened Start Mode: Manual,	
Enterprise App Management (EntAppSvc) Service (Hardened Start	
Extensible Authentication Protocol Service (Hardened Start Mode:	
Function Discovery Provider Host Service (Hardened Start Mode:	
Function Discovery Resource Publication Service (Hardened Start	
Geolocation (lfsvc) Service (Hardened Start Mode: Disabled, Hardened	
Group Policy Client Service (Hardened Start Mode: Auto, Hardened	
Human Interface Device Access Service (Hardened Start Mode:	
HV Host (HvHost) Service (Hardened Start Mode: Manual, Hardened	
Hyper-V Data Exchange Service (vmickvpexchange) Service (Hardened	
Hyper-V Guest Service Interface (vmicguestinterface) Service	
Hyper-V Guest Shutdown Service (vmicshutdown) Service (Hardened	
Hyper-V Heartbeat Service (vmicheartbeat) Service (Hardened Start	
Hyper-V PowerShell Direct Service (vmicvmsession) Service (Hardened	
Hyper-V Remote Desktop Virtualization Service (vmicrdv) Service	
Hyper-V Time Synchronization Service (vmictimesync) Service	
Hyper-V Volume Shadow Copy Requestor (vmicvss) Service (Hardened	
IKE and AuthIP IPsec Keying Modules Service (Hardened Start Mode:	Fail: state IKEEXT (running), startmode IKEEXT (auto).
Interactive Services Detection Service (Hardened Start Mode: Disabled,	
Internet Connection Sharing (ICS) Service (Hardened Start Mode:	
IP Helper Service (Hardened Start Mode: Disabled, Hardened Expected	Fail: state iphlpsvc (running), startmode iphlpsvc (auto).
IPsec Policy Agent Service (Hardened Start Mode: Manual, Hardened	
KDC Proxy Server service (KPSSVC) Service (Hardened Start Mode:	
KtmRm for Distributed Transaction Coordinator Service (Hardened Start	
Link-Layer Topology Discovery Mapper Service (Hardened Start Mode:	
Local Session Manager Service (Hardened Start Mode: Automatic,	
Microsoft (R) Diagnostics Hub Standard Collector Service	
Microsoft App-V Client Service (Hardened Start Mode: Disabled,	
Microsoft Account Sign-in Assistant Service (Hardened Start Mode:	

Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mandatory Services

Rule Name	Result
Microsoft iSCSI Initiator Service (Hardened Start Mode: Disabled,	Fail: state MSiSCSI (stopped), startmode MSiSCSI (manual).
Microsoft Passport (NgcSvc) Service (Hardened Start Mode: Disabled,	Fail: state NgcSvc (stopped), startmode NgcSvc (manual).
Microsoft Passport Container (NgcCtnrSvc) Service (Hardened Start	Fail: state NgcCtnrSvc (stopped), startmode NgcCtnrSvc (manual).
Microsoft Software Shadow Copy Provider Service (Hardened Start	
Microsoft Storage Spaces SMP (smphost) Service (Hardened Start	
Net.Tcp Port Sharing Service (Hardened Start Mode: Disabled,	
Netlogon Service (Hardened Start Mode: Manual, Hardened Expected	
Network Access Protection Agent Service (Hardened Start Mode:	

Network Connections Service (Hardened Start Mode: Manual,	
Network Connectivity Assistant (ncasvc) Service (Hardened Start Mode:	
Network List Service (Hardened Start Mode: Manual, Hardened	
Network Location Awareness Service (Hardened Start Mode: Auto,	
Network Setup (NetSetupSvc) Service (Hardened Start Mode: Manual,	
Network Store Interface Service (Hardened Start Mode: Auto, Hardened	
Offline Files (CscService) Service (Hardened Start Mode: Disabled,	
Optimize Drives (defragsvc) Service (Hardened Start Mode: Manual,	
Performance Counter DLL Host (PerfHost) Service (Hardened Start	
Performance Logs and Alerts Service (Hardened Start Mode: Manual,	
Phone (PhoneSvc) Service (Hardened Start Mode: Disabled, Hardened	
Plug and Play Service (Hardened Start Mode: Manual, Hardened	
Portable Device Enumerator (WPDBusEnum) Service Hardened Start	
Power Service (Hardened Start Mode: Auto, Hardened Expected State:	
Print Spooler Service (Hardened Start Mode: Disabled, Hardened	
Printer Extensions and Notifications (PrintNotify) Service (Hardened	
Problem Reports and Solutions Control Panel Support Service	
Program Compatibility Assistant (PcaSvc) Service (Hardened Start	
Quality Windows Audio Video Experience (QWAVE) Service (Hardened	
Radio Management Service (RmSvc) Service (Hardened Start Mode:	
Remote Access Auto Connection Manager Service (Hardened Start	
Remote Access Connection Manager Service (Hardened Start Mode:	
Remote Desktop Configuration Service (Hardened Start Mode:	Fail: state SessionEnv (running), startmode SessionEnv (manual).
Remote Desktop Services Service (Hardened Start Mode: Disabled,	Fail: state TermService (running), startmode TermService (manual).
Remote Desktop Services UserMode Port Redirector (Hardened Start	Fail: state UmRdpService (running), startmode UmRdpService (manual).
Remote Procedure Call (RPC) Service (Hardened Start Mode: Auto,	
Remote Procedure Call (RPC) Locator Service (Hardened Start Mode:	
Remote Registry Service (Hardened Start Mode: Disabled, Hardened	Fail: state RemoteRegistry (stopped), startmode RemoteRegistry (auto).
Resultant Set of Policy Provider Service (Hardened Start Mode:	
Routing and Remote Access Service (Hardened Start Mode: Disabled,	
RPC Endpoint Mapper Service (Hardened Start Mode: Auto, Hardened	
Secondary Logon Service (Hardened Start Mode: Manual, Hardened	
Secure Socket Tunneling Protocol Service (Hardened Start Mode:	
Security Accounts Manager Service (Hardened Start Mode: Auto,	
Sensor Data Service (SensorDataService) Service (Hardened Start	
Sensor Monitoring Service (SensrSvc) Service (Hardened Start Mode:	
Sensor Service (SensorService) Service (Hardened Start Mode:	
Server Service (Hardened Start Mode: Disabled, Hardened Expected	Fail: state LanmanServer (running), startmode LanmanServer (auto).

Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mandatory Services

Rule Name	**Result**
Shell Hardware Detection Service (Hardened Start Mode: Auto,	
Smart Card Service (Hardened Start Mode: Disabled, Hardened	
Smart Card Device Enumeration (ScDeviceEnum) Service (Hardened	
Smart Card Removal Policy (SCPolicySvc) Service (Hardened Start	
SNMP Trap Service (Hardened Start Mode: Disabled, Hardened	Fail: state SNMPTRAP (stopped), startmode SNMPTRAP (manual).
Software Protection Service (Hardened Start Mode: Auto, Hardened	
Special Administration Console Helper Service (Hardened Start Mode:	Fail: state sacsvr (stopped), startmode sacsvr (disabled).
Spot Verifier Service (Hardened Start Mode: Manual, Hardened	
SSDP Discovery Service (Hardened Start Mode: Disabled, Hardened	
State Repository (StateRepository) Service (Hardened Start Mode:	
Still Image Acquisition Events (WiaRpc) Service (Hardened Start Mode:	
Storage (StorSvc) Service (Hardened Start Mode: Manual, Hardened	
Storage Tiers Management Service (Hardened Start Mode: Manual,	

Superfetch Service (Hardened Start Mode: Disabled, Hardened	
Sync Host (OneSyncSvc) Service (Hardened Start Mode: Disabled,	
System Event Notification Service (Hardened Start Mode: Auto,	
System Events Broker Service (Hardened Start Mode: Auto, Hardened	
Task Scheduler Service (Hardened Start Mode: Auto, Hardened	
TCP/IP NetBIOS Helper Service (Hardened Start Mode: Manual,	
Telephony Service (Hardened Start Mode: Disabled, Hardened	
Themes Service (Hardened Start Mode: Disabled, Hardened Expected	
Tile Data model server Service (Hardened Start Mode: Auto, Hardened	
Time Broker (TimeBrokerSvc) Service (Hardened Start Mode: Manual,	
Touch Keyboard and Handwriting Panel Service (Hardened Start Mode:	
Update Orchestrator Service for Windows Update (UsoSvc) Service	
UPnP Device Host Service (Hardened Start Mode: Disabled, Hardened	
User Access Logging Service (Hardened Start Mode: Auto, Hardened	
User Data Access (UserDataSvc) Service (Hardened Start Mode:	
User Data Storage (UnistoreSvc) Service (Hardened Start Mode:	
User Experience Virtualization (UevAgentService) Service (Hardened	
User Manager (UserManager) Service (Hardened Start Mode: Auto,	
User Profile (ProfSvc) Service (Hardened Start Mode: Auto, Hardened	
Virtual Disk Service (Hardened Start Mode: Manual, Hardened	
Volume Shadow Copy Service (Hardened Start Mode: Manual,	
WalletService (WalletService) Service (Hardened Start Mode: Disabled,	
Windows Audio Service (Hardened Start Mode: Disabled, Hardened	
Windows Audio Endpoint Builder Service (Hardened Start Mode:	
Windows Biometric Service (Hardened Start Mode: Disabled, Hardened	
Windows Connection Manager (wcmsvc) Service (Hardened Start	
Windows Camera Frame (FrameServer) Service (Hardened Start Mode:	
Windows Defender Network Inspection (WdNisSvc) Service (Hardened	
Windows Defender (WinDefend) Service (Hardened Start Mode: Auto,	
Windows Driver Foundation - User-mode Driver Framework (wudfsvc)	
Windows Encryption Provider Host (WEPHOSTSVC) Service	
Windows Error Reporting (WerSvc) Service (Hardened Start Mode:	Fail: state WerSvc (stopped), startmode WerSvc (manual).
Windows Event Collector (Wecsvc) Service (Hardened Start Mode:	Fail: state Wecsvc (stopped), startmode Wecsvc (manual).

Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mandatory Services

Rule Name	Result
Windows Event Log (EventLog) Service (Hardened Start Mode: Auto,	
Windows Firewall (MpsSvc) Service (Hardened Start Mode: Auto,	
Windows Font Cache (FontCache) Service (Hardened Start Mode:	
Windows Image Acquisition (WIA) (stisvc) Service (Hardened Start	
Windows Insider (wisvc) Service (Hardened Start Mode: Disabled,	
Windows Installer Service (Hardened Start Mode: Manual, Hardened	
Windows License Manager (LicenseManager) Service (Hardened Start	
Windows Management Instrumentation Service (Hardened Start Mode:	
Windows Mobile Hotspot Service (icssvc) Service (Hardened Start	Fail: state icssvc (stopped), startmode icssvc (manual).
Windows Modules Installer Service (Hardened Start Mode: Manual,	
Windows Push Notifications System (WpnService) Service (Hardened	Fail: state WpnService (running), startmode WpnService (auto).
Windows Push Notifications User (WpnUserService) Service (Hardened	
Windows Presentation Foundation Font Cache (FontCache3.0.0.0)	
Windows Remote Management (WS-Management) Service (Hardened	Fail: state WinRM (running), startmode WinRM (auto).
Windows Search (WSearch) Service (Hardened Start Mode: Disabled,	
Windows Time Service (Hardened Start Mode: Auto, Hardened	
Windows Update Service (Hardened Start Mode: Manual, Hardened	
WinHTTP Web Proxy Auto-Discovery (WinHttpAutoProxySvc) Service	Fail: state WinHttpAutoProxySvc (running), startmode WinHttpAutoProxySvc (manual).

Wired AutoConfig Service (Hardened Start Mode: Disabled, Hardened	Fail: state dot3svc (stopped), startmode dot3svc (manual).
WMI Performance Adapter Service (Hardened Start Mode: Manual,	
Workstation Service (Hardened Start Mode: Auto, Hardened Expected	
Xbox Live Auth Manager (XblAuthManager) Service (Hardened Start	Fail: state XblAuthManager (stopped), startmode XblAuthManager (manual).
Xbox Live Game Save (XblGameSave) Service (Hardened Start Mode:	Fail: state XblGameSave (stopped), startmode XblGameSave (manual).

HIPAA Standard: Optional Services List - 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

Optional Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Optional Services

Rule Name	Result
Optional Services List: NNT ChangeTracker Gen7 Agent (Gen7Agent)	
Optional Services List: NNT Change Tracker Gen 7 MongoDB Service	
Optional Services List: NNT Change Tracker Gen 7 Redis Service	
Optional Services List: ASP.NET State Service (aspnet_state) Service	Fail: state aspnet_state (stopped), startmode aspnet_state (2 items: manual, manual).
Optional Services List: World Wide Web Publishing Service (Hardened	Fail: This rule checks that the World Wide Web Publishing Service (W3SVC) is in one of the following states: 'stopped' and start mode is: 'Disabled':
Optional Services List: W3C Logging Service (Hardened Start Mode:	Fail: This rule checks that the World Wide Web Publishing Service (W3SVC) is in one of the following states: 'stopped' and start mode is: 'Disabled':

4.12. Workstation Security (§ 164.310(c))

HIPAA Standard: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Identify All Methods of Physical Access to Workstations, Analyze the Risk Associated with Each Type of Access, Identify and Implement Physical Safeguards for Workstations

Rule Name	Result
Document the different ways workstations are accessed by employees	Pass: This rule is not automatically assessed. Document the different ways workstations are accessed by employees and nonemployees, Determine which

4.13. Device and Media Controls (§ 164.310(d)(1))

HIPAA Standard: 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

Implement Procedures for Reuse of Electronic Media - Security parameters to prevent misuse: Account Policies - Devices Rules

Rule Name	Result
Ensure 'Devices: Allowed to format and eject removable media' is set to	Fail: FAILED: (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' : .''. Remediation : To establish the recommended
Ensure 'Devices: Prevent users from installing printer drivers' is set to	Pass: PASSED: '1'.

4.14. Access Control (§ 164.312(a)(1))

HIPAA Standard: 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

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Firewall configuration standards: Windows Firewall With Advanced Security - Domain

Rule Name	Result
Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' : .'0'. Remediation : To establish the recommended
Ensure 'Windows Firewall: Domain: Inbound connections' is set to	Pass: PASSED: '1'.
Ensure 'Windows Firewall: Domain: Outbound connections' is set to	Pass: PASSED: '0'.
Ensure 'Windows Firewall: Domain: Settings: Display a notification' is	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' : .'0'. Remediation : To establish the recommended
Set 'Windows Firewall: Domain: Allow unicast response' to 'No'	Fail: Set 'Windows Firewall: Domain: Allow unicast response' to 'No' : .'0'. Remediation : To establish the recommended configuration via GP, set the
Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules'	Pass: PASSED: '1'.
Ensure 'Windows Firewall: Domain: Settings: Apply local connection	Pass: PASSED: '1'.
Ensure 'Windows Firewall: Domain: Logging: Name' is set to	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to 'C:\Windows\System32\logfiles\firewall\domainfw.log' : .''. Remediation : To
Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' : .'0'. Remediation : To establish the
Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' : .''. Remediation : To establish the recommended
Ensure 'Windows Firewall: Domain: Logging: Log successful	Fail: FAILED: (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' : .''. Remediation : To establish the recommended

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Firewall configuration standards: Windows Firewall With Advanced Security - Private Profile

Rule Name	Result
Ensure 'Windows Firewall: Private: Firewall state' is set to 'On	Fail: FAILED: (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' : .'0'. Remediation : To establish the recommended
Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block	Pass: PASSED: '1'.
Ensure 'Windows Firewall: Private: Outbound connections' is set to	Pass: PASSED: '0'.
Ensure 'Windows Firewall: Private: Settings: Display a notification' is set	Fail: FAILED: (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' : .'0'. Remediation : To establish the recommended
Set 'Windows Firewall: Private: Allow unicast response' to 'No'	Fail: Set 'Windows Firewall: Private: Allow unicast response' to 'No' : .'0'. Remediation : To establish the recommended configuration via GP, set the
Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is	Pass: PASSED: '1'.
Ensure 'Windows Firewall: Private: Settings: Apply local connection	Pass: PASSED: '1'.

Ensure 'Windows Firewall: Private: Logging: Name' is set to	Fail: FAILED: (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to 'C:\Windows\System32\logfiles\firewall\privatefw.log' : .''. Remediation : To
Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to	Fail: FAILED: (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' : .'0'. Remediation : To establish the
Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is	Fail: FAILED: (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' : .''. Remediation : To establish the recommended
Ensure 'Windows Firewall: Private: Logging: Log successful	Fail: FAILED: (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' : .''. Remediation : To establish the recommended

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Firewall configuration standards: Windows Firewall With Advanced Security - Public Profile

Rule Name	**Result**
Ensure 'Windows Firewall: Public: Firewall state' is set to 'On	Fail: FAILED: (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' : .'0'. Remediation : To establish the recommended
Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block	Pass: PASSED: '1'.
Ensure 'Windows Firewall: Public: Outbound connections' is set to	Pass: PASSED: '0'.
Ensure 'Windows Firewall: Public: Settings: Display a notification' is set	Pass: PASSED: '0'.
Set 'Windows Firewall: Public: Allow unicast response' to 'No'	Fail: Set 'Windows Firewall: Public: Allow unicast response' to 'No' : .'0'. Remediation : To establish the recommended configuration via GP, set the following
Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is	Fail: FAILED: (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' : .'1'. Remediation : To establish the recommended
Ensure 'Windows Firewall: Public: Settings: Apply local connection	Fail: FAILED: (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' : .'1'. Remediation : To establish the
Ensure 'Windows Firewall: Public: Logging: Name' is set to	Fail: FAILED: (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to 'C:\Windows\System32\logfiles\firewall\publicfw.log' : .''. Remediation : To
Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to	Fail: FAILED: (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' : .'0'. Remediation : To establish the
Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set	Fail: FAILED: (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' : .''. Remediation : To establish the recommended
Ensure 'Windows Firewall: Public: Logging: Log successful	Fail: FAILED: (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' : .''. Remediation : To establish the recommended

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Security parameters to prevent misuse: Account Policies - Security Options

Rule Name	Result
Ensure 'Accounts: Administrator account status' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' : . Remediation : To establish the recommended configuration via GP,
Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add	Fail: FAILED: (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' : .''. Remediation : To establish
Ensure 'Accounts: Guest account status' is set to 'Disabled'	Pass: PASSED:.
Ensure 'Accounts: Limit local account use of blank passwords to	Pass: PASSED: '1'.
Configure 'Accounts: Rename administrator account'	Fail: FAILED: (L1) Configure 'Accounts: Rename administrator account' : securitypolicy (2 items: "Administrator", "Administrator"). Remediation : To establish
Configure 'Accounts: Rename guest account'	Fail: FAILED: (L1) Configure 'Accounts: Rename guest account' : securitypolicy (2 items: "Guest", "Guest"). Remediation : To establish the recommended

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Network Access Rules

Rule Name	Result
Ensure 'Network access: Allow anonymous SID/Name translation' is set	Pass: PASSED:.
Ensure 'Network access: Do not allow anonymous enumeration of SAM	Pass: PASSED: '1'.
Ensure 'Network access: Do not allow anonymous enumeration of SAM	Fail: FAILED: (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) : .'0'.
Ensure 'Network access: Do not allow storage of passwords and	Fail: FAILED: (L2) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' : .'0'.
Ensure 'Network access: Let Everyone permissions apply to	Pass: PASSED: '0'.
Configure 'Network access: Named Pipes that can be accessed	Pass: PASSED: ' '.
Configure 'Network access: Remotely accessible registry paths'	Pass: PASSED: securitypolicy (3 items: SYSTEM\CURRENTCONTROLSET\CONTROL\PRODUCTOPTIONS,
Configure 'Network access: Remotely accessible registry paths and sub-	Pass: PASSED: securitypolicy (11 items: SYSTEM\CURRENTCONTROLSET\CONTROL\PRINT\PRINTERS,
Ensure 'Network access: Restrict anonymous access to Named Pipes	Pass: PASSED: '1'.
Ensure 'Network access: Restrict clients allowed to make remote calls	Fail: FAILED: (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only)
Ensure 'Network access: Shares that can be accessed anonymously' is	Pass: PASSED: ''.
Ensure 'Network access: Sharing and security model for local accounts'	Pass: PASSED: '0'.

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Network Security Rules

Rule Name	Result
Ensure 'Do not display network selection UI' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Do not display network selection UI' is set to 'Enabled' : .''. Remediation : To implement the recommended configuration state, set
Ensure 'Do not enumerate connected users on domain-joined	Fail: FAILED: (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' : .''. Remediation : To establish the
Ensure 'Enumerate local users on domain-joined computers' is set to	Fail: FAILED: (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' : .''. Remediation : To establish the recommended
Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' : .''. Remediation : To establish the recommended configuration via GP,
Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' : .''. Remediation : To establish the recommended configuration via
Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to	Fail: FAILED: (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) : .''. Remediation : To establish the
Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled:	Fail: FAILED: (L2) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) : .''. Remediation : To establish the
Ensure 'Network security: Allow Local System to use computer identity	Fail: FAILED: (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' : .''. Remediation : To establish the
Ensure 'Network security: Allow LocalSystem NULL session fallback' is	Fail: FAILED: (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' : .''. Remediation : To establish the recommended
Ensure 'Network Security: Allow PKU2U authentication requests to this	Fail: FAILED: (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' : .''.
Ensure 'Network security: Configure encryption types allowed for	Fail: FAILED: (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1,
Ensure 'Support device authentication using certificate' is set to	Fail: FAILED: (L2) Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' : False.''. Remediation : To establish the
Ensure 'Network security: Do not store LAN Manager hash value on	Pass: PASSED: '1'.
Configure 'Deny access to this computer from the network'	Fail: FAILED: (L1) Configure 'Deny access to this computer from the network' : securitypolicy (). Remediation : To establish the recommended configuration
Ensure 'Deny log on as a batch job' to include 'Guests'	Fail: FAILED: (L1) Ensure 'Deny log on as a batch job' to include 'Guests' : securitypolicy (). Remediation : To establish the recommended configuration via
Ensure 'Deny log on as a service' to include 'Guests'	Fail: FAILED: (L1) Ensure 'Deny log on as a service' to include 'Guests' : securitypolicy (). Remediation : To establish the recommended configuration via
Ensure 'Deny log on locally' to include 'Guests'	Fail: FAILED: (L1) Ensure 'Deny log on locally' to include 'Guests' : securitypolicy (). Remediation : To establish the recommended configuration via GP, set
Ensure 'Deny log on through Remote Desktop Services' to include	Fail: FAILED: (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' : securitypolicy (). Remediation : To establish
Set 'NetBIOS node type' to 'P-node' (Ensure NetBT Parameter	Fail: FAILED: (L1) Set 'NetBIOS node type' to 'P-node' (Ensure NetBT Parameter 'NodeType' is set to '0x2 (2)') (MS Only) : .''. Remediation : To establish the
Ensure 'Turn off multicast name resolution' is set to 'Enabled' (MS Only)	Fail: FAILED: (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (MS Only) : .''. Remediation : To establish the recommended configuration
Ensure 'Enable Font Providers' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Enable Font Providers' is set to 'Disabled' : .''. Remediation : To establish the recommended configuration via GP, set the
Ensure 'Enable insecure guest logons' is set to 'Disabled'	Fail: FAILED: (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled' : .''. Remediation : To establish the recommended configuration via GP, set the

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Network Security Rules

Rule Name	Result
Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' : False.''. Remediation : To implement the recommended configuration
Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' : False.''. Remediation : To implement the recommended configuration
Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to	Fail: FAILED: (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' : .''. Remediation : To establish the recommended

Ensure 'Prohibit installation and configuration of Network Bridge on your	Fail: FAILED: (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' : .''. Remediation : To
Ensure 'Prohibit use of Internet Connection Sharing on your DNS	Fail: FAILED: (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' : .''. Remediation : To establish the
Ensure 'Require domain users to elevate when setting a network's	Fail: FAILED: (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' : .''. Remediation : To establish the
Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive	Fail: FAILED: (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' : .''.
Ensure 'Enable/Disable PerfTrack' is set to 'Disabled'	Fail: FAILED: (L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' : .''. Remediation : To establish the recommended configuration via GP, set the
Ensure 'Use enhanced anti-spoofing when available' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Use enhanced anti-spoofing when available' is set to 'Enabled' : .''. Remediation : To establish the recommended configuration
Ensure 'Restrict Remote Desktop Services users to a single Remote	Fail: FAILED: (L2) Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' : .''. Remediation : To
Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	Fail: FAILED: (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' : .''. Remediation : To establish the recommended configuration via GP, set

4.15. Audit Controls (§ 164.312(b))

HIPAA Standard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information

Select the Tools that Will Be Deployed for Auditing and System Activity Reviews

Rule Name	Result
Configure 'Manage auditing and security log'	Pass: PASSED: securitypolicy (BUILTIN\ADMINISTRATORS).
Ensure 'Generate security audits' is set to 'LOCAL SERVICE,	Fail: FAILED: (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' : securitypolicy (4 items: IIS APPPOOL\NNT WEB
Ensure 'Audit: Force audit policy subcategory settings (Windows Vista	Fail: FAILED: (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'
Ensure 'Audit: Shut down system immediately if unable to log security	Pass: PASSED: '0'.

Develop Appropriate Standard Operating Procedures: Windows Components - Event Log Rules

Rule Name	Result
Ensure 'Application: Control Event Log behavior when the log file	Fail: FAILED: (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' : .''. Remediation : To
Ensure 'Application: Specify the maximum log file size (KB)' is set to	Fail: FAILED: (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' : .'0'. Remediation : To establish the
Ensure 'Security: Control Event Log behavior when the log file reaches	Fail: FAILED: (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' : .''. Remediation : To
Ensure 'Security: Specify the maximum log file size (KB)' is set to	Fail: FAILED: (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' : .'0'. Remediation : To establish the
Ensure 'Setup: Control Event Log behavior when the log file reaches its	Fail: FAILED: (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' : .''. Remediation : To establish
Ensure 'Setup: Specify the maximum log file size (KB)' is set to	Fail: FAILED: (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' : .'0'. Remediation : To establish the
Ensure 'System: Control Event Log behavior when the log file reaches	Fail: FAILED: (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' : .''. Remediation : To
Ensure 'System: Specify the maximum log file size (KB)' is set to	Fail: FAILED: (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' : .'0'. Remediation : To establish the

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - System Rules

Rule Name	Result
Ensure 'Audit System Integrity' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via GP, set
Ensure 'Audit Security System Extension' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via
Ensure 'Audit Security State Change' is set to 'Success' (CCE	Fail: FAILED: (L1) Ensure 'Audit Security State Change' is set to 'Success' : . Remediation : To establish the recommended configuration via GP, set the
Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via GP, set the
Ensure 'Audit Other System Events' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via GP,

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Object Access Rules

Rule Name	Result
Set 'Audit Policy: Object Access: Handle Manipulation' to 'No Auditing'	Pass: Rule passed :.
Set 'Audit Policy: Object Access: Other Object Access Events' to 'No	Pass: Rule passed :.
Set 'Audit Policy: Object Access: File Share' to 'No Auditing'	Pass: Rule passed :.
Set 'Audit Policy: Object Access: File System' to 'No Auditing'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to No Auditing. Computer
Set 'Audit Policy: Object Access: SAM' to 'No Auditing'	Pass: Rule passed :.
Set 'Audit Policy: Object Access: Kernel Object' to 'No Auditing'	Pass: Rule passed :.
Set 'Audit Policy: Object Access: Filtering Platform Packet Drop' to 'No	Pass: Rule passed :.
Set 'Audit Policy: Object Access: Registry' to 'No Auditing'	Fail: Remediation : To implement the recommended configuration state, set the following Group Policy setting to No Auditing. Computer
Set 'Audit Policy: Object Access: Certification Services' to 'No Auditing'	Pass: Rule passed :.
Set 'Audit Policy: Object Access: Application Generated' to 'No Auditing'	Pass: Rule passed :.
Set 'Audit Policy: Object Access: Detailed File Share' to 'No Auditing'	Pass: Rule passed :.
Set 'Audit Policy: Object Access: Filtering Platform Connection' to 'No	Pass: Rule passed :.
Ensure 'Audit Removable Storage' is set to 'Success and Failure'	Fail: (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via GP, set the

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Logon-Logoff Rules

Rule Name	Result
Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via
Ensure 'Audit Special Logon' is set to 'Success'	Fail: FAILED: (L1) Ensure 'Audit Special Logon' is set to 'Success' : . Remediation : To establish the recommended configuration via GP, set the following UI
Set 'Audit Policy: Logon-Logoff: IPsec Main Mode' to 'No Auditing'	Pass: Rule passed :.
Ensure 'Audit Account Lockout' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit Account Lockout' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via GP, set
Ensure 'Audit Group Membership' is set to 'Success'	Fail: FAILED: (L1) Ensure 'Audit Group Membership' is set to 'Success' : . Remediation : To establish the recommended configuration via GP, set the
Set 'Audit Policy: Logon-Logoff: IPsec Extended Mode' to 'No Auditing'	Pass: Rule passed :.
Set 'Audit Policy: Logon-Logoff: IPsec Quick Mode' to 'No Auditing'	Pass: Rule passed :.
Ensure 'Audit Logoff' is set to 'Success'	Fail: FAILED: (L1) Ensure 'Audit Logoff' is set to 'Success' : . Remediation : To establish the recommended configuration via GP, set the following UI path to
Set 'Audit Policy: Logon-Logoff: Network Policy Server' to 'No Auditing'	Pass: Rule passed :.
Ensure 'Audit Logon' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit Logon' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via GP, set the

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - DS Access Rules

Rule Name	Result
Set 'Audit Policy: DS Access: Directory Service Replication' to 'No	Pass: Rule passed :.
Set 'Audit Policy: DS Access: Detailed Directory Service Replication' to	Pass: Rule passed :.
Set 'Audit Policy: DS Access: Directory Service Changes' to 'No	Pass: Rule passed :.
Set 'Audit Policy: DS Access: Directory Service Access' to 'No Auditing'	Pass: Rule passed :.

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Detailed Tracking Rules

Rule Name	Result
Set 'Audit Policy: Detailed Tracking: DPAPI Activity' to 'No Auditing'	Pass: Rule passed :.
Set 'Audit Policy: Detailed Tracking: Process Termination' to 'No	Pass: Rule passed :.
Ensure 'Audit PNP Activity' is set to 'Success'	Fail: FAILED: (L1) Ensure 'Audit PNP Activity' is set to 'Success' : . Remediation : To establish the recommended configuration via GP, set the following UI
Ensure 'Audit Process Creation' is set to 'Success' (CCE Reference :	Fail: FAILED: (L1) Ensure 'Audit Process Creation' is set to 'Success' : . Remediation : To establish the recommended configuration via GP, set the following
Set 'Audit Policy: Detailed Tracking: RPC Events' to 'No Auditing'	Pass: Rule passed :.

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Policy Change Rules

Rule Name	Result
Set 'Audit Policy: Policy Change: MPSSVC Rule-Level Policy Change'	Pass: Rule passed :.
Set 'Audit Policy: Policy Change: Filtering Platform Policy Change' to	Pass: Rule passed :.
Ensure 'Audit Authorization Policy Change' is set to 'Success'	Fail: FAILED: (L1) Ensure 'Audit Authorization Policy Change' is set to 'Success' : . Remediation : To establish the recommended configuration via GP, set
Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via GP,
Set 'Audit Policy: Policy Change: Other Policy Change Events' to 'No	Pass: Rule passed :.
Ensure 'Audit Authentication Policy Change' is set to 'Success'	Fail: FAILED: (L1) Ensure 'Audit Authentication Policy Change' is set to 'Success' : . Remediation : To establish the recommended configuration via GP, set

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Account Management Rules

Rule Name	Result
Set 'Audit Policy: Account Management: Distribution Group	Pass: Rule passed :.
Ensure 'Audit Computer Account Management' is set to 'Success and	Fail: FAILED: (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure' : . Remediation : To establish the recommended
Ensure 'Audit User Account Management' is set to 'Success and	Fail: FAILED: (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration
Ensure 'Audit Security Group Management' is set to 'Success and	Fail: FAILED: (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration
Ensure 'Audit Other Account Management Events' is set to 'Success	Fail: FAILED: (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' : . Remediation : To establish the recommended
Ensure 'Audit Application Group Management' is set to 'Success and	Fail: FAILED: (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure' : . Remediation : To establish the recommended

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Account Logon Rules

Rule Name	Result
Set 'Audit Policy: Account Logon: Kerberos Authentication Service' to	Pass: Rule passed :.
Set 'Audit Policy: Account Logon: Other Account Logon Events' to 'No	Pass: Rule passed :.
Set 'Audit Policy: Account Logon: Kerberos Service Ticket Operations'	Pass: Rule passed :.
Ensure 'Audit Credential Validation' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via GP,

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Privilege Use Rules

Rule Name	Result
Set 'Audit Policy: Privilege Use: Other Privilege Use Events' to 'No	Pass: Rule passed :.
Set 'Audit Policy: Privilege Use: Non Sensitive Privilege Use' to 'No	Pass: Rule passed :.
Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	Fail: FAILED: (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' : . Remediation : To establish the recommended configuration via

4.16. Integrity (§ 164.312(c)(1))

HIPAA Standard: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Develop and Implement the Integrity Policy and Requirements: Anti-Virus Protection Check

Rule Name	Result
Verify Virus Protection is enabled and updated	Pass: This rule is not automatically assessed. Once you have selected an AV system please contact NNT to incorporate checks for associated AV services

Develop and Implement the Integrity Policy and Requirements: Protect all systems against malware - Early Launch Antimalware Rules

Rule Name	Result
Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good,	Fail: FAILED: (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' : .''. Remediation : To establish the

Develop and Implement the Integrity Policy and Requirements: Protect all systems against malware - Attachment Rules

Rule Name	Result
Ensure 'Notify antivirus programs when opening attachments' is set to	Fail: FAILED: (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' : .''. Remediation : To establish the recommended

5 - 6. Implement a Mechanism to Authenticate EPHI and a Monitoring Process To Assess How the Implemented Process Is Working

Rule Name	Result
Implement electronic mechanisms to corroborate that EPHI has not	Pass: This rule is not automatically assessed. Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an

4.17. Person or Entity Authentication (§ 164.312(d))

HIPAA Standard: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Authentication - Security parameters to prevent misuse: Account Policies - Interactive logon Rules

Rule Name	Result
Ensure 'Interactive logon: Do not display last user name' is set to	Fail: FAILED: (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' : .'0'. Remediation : To establish the recommended
Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to	Pass: PASSED: '0'.
Configure 'Interactive logon: Message text for users attempting to log	Fail: FAILED: (L1) Configure 'Interactive logon: Message text for users attempting to log on' : securitypolicy ().''. Remediation : To establish the
Configure 'Interactive logon: Message title for users attempting to log	Fail: FAILED: (L1) Configure 'Interactive logon: Message title for users attempting to log on' : securitypolicy ("").'"". Remediation : To establish the
Ensure 'Interactive logon: Number of previous logons to cache (in case	Fail: FAILED: (L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)'
Ensure 'Interactive logon: Prompt user to change password before	Pass: PASSED: True'5'.
Ensure 'Interactive logon: Require Domain Controller Authentication to	Fail: FAILED: (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) : .'0'. Remediation
Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock	Fail: FAILED: (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher : .'0'. Remediation : To establish the

Authentication - Security parameters to prevent misuse: Account Policies - MSS Rules

Rule Name	Result
Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not	Fail: FAILED: (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' : .''. Remediation : To establish the
Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing	Fail: FAILED: (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled:
Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection	Fail: FAILED: (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest
Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override	Fail: FAILED: (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' : .'1'. Remediation : To
Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent	Fail: FAILED: (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes
Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to	Fail: FAILED: (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is
Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and	Fail: FAILED: (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to
Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode	Fail: FAILED: (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' : .''. Remediation : To establish the
Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times	Fail: FAILED: (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' : .''.
Ensure 'MSS: (TcpMaxDataRetransmissions) How many times	Fail: FAILED: (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' : .''.
Ensure 'MSS: (WarningLevel) Percentage threshold for the security	Fail: FAILED: (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to

Authentication - Security parameters to prevent misuse: Account Policies - Recovery console Rules

Rule Name	Result
Set 'Recovery console: Allow automatic administrative logon' to	Pass: Rule passed : '0'.
Set 'Recovery console: Allow floppy copy and access to all drives and	Pass: Rule passed : '0'.

Authentication -Security parameters to prevent misuse: Account Policies - Shutdown Rules

Rule Name	Result
Ensure 'Shutdown: Allow system to be shut down without having to log	Pass: PASSED: '0'.

Authentication -Security parameters to prevent misuse: Account Policies - System objects Rules

Rule Name	Result
Ensure 'System objects: Require case insensitivity for non-Windows	Pass: PASSED: '1'.
Ensure 'System objects: Strengthen default permissions of internal	Pass: PASSED: '1'.

4.18. Transmission Security (§ 164.312(e)(1))

HIPAA Standard: 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.

Transmission Security - Security parameters to prevent misuse: Account Policies - Domain member Rules

Rule Name	Result
Ensure 'Domain member: Digitally encrypt or sign secure channel data	Pass: PASSED: '1'.
Ensure 'Domain member: Digitally encrypt secure channel data (when	Pass: PASSED: '1'.
Ensure 'Domain member: Digitally sign secure channel data (when	Pass: PASSED: '1'.
Ensure 'Domain member: Disable machine account password changes'	Pass: PASSED: '0'.
Ensure 'Domain member: Maximum machine account password age' is	Pass: PASSED: True'30'.
Ensure 'Domain member: Require strong (Windows 2000 or later)	Pass: PASSED: '1'.

Transmission Security - Security parameters to prevent misuse: Account Policies - Microsoft network client Rules

Rule Name	Result
Ensure 'Microsoft network client: Digitally sign communications	Fail: FAILED: (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' : .'0'. Remediation : To establish the
Ensure 'Microsoft network client: Digitally sign communications (if	Pass: PASSED: '1'.
Ensure 'Microsoft network client: Send unencrypted password to third-	Pass: PASSED: '0'.

Transmission Security - Security parameters to prevent misuse: Account Policies - Microsoft network server Rules

Rule Name	Result
Ensure 'Microsoft network server: Digitally sign communications	Fail: FAILED: (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' : .'0'. Remediation : To establish the
Ensure 'Microsoft network server: Digitally sign communications (if	Fail: FAILED: (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' : .'0'. Remediation : To establish the
Ensure 'Microsoft network server: Server SPN target name validation	Fail: FAILED: (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) : .'0'.

Transmission Security - Use strong cryptography and security protocols

Rule Name	Result
Ensure 'System cryptography: Force strong key protection for user keys	Fail: (L2) Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User is prompted when the key is first
Set 'System cryptography: Use FIPS compliant algorithms for	Fail: Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled' : .'0'.
Ensure 'Network security: LAN Manager authentication level' is set to	Fail: FAILED: (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM&NTLM' : .''. Remediation :
Ensure 'Network security: LDAP client signing requirements' is set to	Pass: PASSED: '1'.
Ensure 'Network security: Minimum session security for NTLM SSP	Fail: FAILED: (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2
Ensure 'Network security: Minimum session security for NTLM SSP	Fail: FAILED: (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2
Ensure 'Domain member: Require strong (Windows 2000 or later)	Pass: PASSED: '1'.