HIPAA Assessment

HIPAA Management Plan

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

Scan Date: 13-Dec-2018

Prepared for:

HIPAA – Covered EntityPrepared by:
AMS Networks

14-Dec-2018

Management Plan

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the global Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the global Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

Risk Score	Recommendation	Severity	Probability
100	**§164.530(b) - Administrative requirements - Standard: Training and Implementation specifications: Training.** Ensure that all workforce members receive training pertaining to the Breach Notification Rule.	H	H
100	**§ 164.520 - Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.** Create an organizational policy requiring that a Notice of Privacy Practices be written to comply with requirements of the HIPAA and HITECH Acts, and be given to all new patients who acknowledge receipt in writing; prominently displayed in patient areas; available to all who request it; and prominently displayed on your website.	H	H
100	**§164.512(e) - Uses and Disclosure - Standard: Disclosures for judicial and administrative proceedings.** Ensure that everyone who may be involved with receiving and responding to law enforcement requests, court orders, and subpoenas (not accompanied by a court order) has been trained and reminded what procedures are to be followed.	H	H
100	**§164.502(e) Uses and disclosures of protected health information, §164.504(e) - Uses and disclosures - organizational requirements, §164.532(d) - Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.** Ensure that all workforce members have been trained and reminded what procedures are to be followed.	H	H

Risk Score	Recommendation	Severity	Probability
100	**§ 164.520 - Notice of Privacy Practices for protected health information.** Create a written policy requiring compliance with all state and federal requirements related to patients accessing their medical records.	H	H
100	**§ 164.522(b) - Rights to request privacy protection for protected health information - Confidential communications requirements.** Implement a written policy to ensure compliance with HIPAA's requirements for confidential communications.	H	H
100	**§ 164.520 - Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.** Ensure that a link to a downloadable Notice of Privacy Practices be displayed prominently on your website.	H	H
100	**§164.508 - Uses and disclosures requiring an opportunity for the individual to agree or to object - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.** Implement a written policy to ensure compliance with HIPAA's requirements for Authorizations for Uses & Disclosures.	H	H
100	**§ 164.502(e) Uses and disclosures of protected health information, § 164.504(e) - Uses and disclosures - organizational requirements, § 164.532(d) - Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.** Ensure that everyone who may be involved with Business Associates have been trained and reminded what procedures are to be followed.	H	H
100	**§164.510(b) - Uses and disclosures for which authorization is required - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.** Ensure that all workforce members have been trained and reminded what procedures are to be followed during emergencies and disasters.	H	H
100	**§164.530(b) - Administrative requirements - Standard: Training and Implementation specifications: Training.**	H	H

Risk Score	Recommendation	Severity	Probability
	Ensure that all workforce members receive training pertaining to the Breach Notification Rule.		
100	**§164.308(b)(1): Business Associate Contracts and Other Arrangements - Covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in §160.103. The covered entity must obtain satisfactory assurance from the business associate that it will appropriately safeguard the information in accordance with §164.314(a)(1) standards.** Acquire Business Associate agreements with Data Centers in use by the company.	H	H
100	**§164.530(b) - Administrative requirements - Standard: Training and Implementation specifications: Training.** Ensure that all applicable workforce members receive training pertaining to the Breach Notification Rule's requirements for a risk assessment.	H	H
100	**§164.308(b)(1): Business Associate Contracts and Other Arrangements - Covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in §160.103. The covered entity must obtain satisfactory assurance from the business associate that it will appropriately safeguard the information in accordance with §164.314(a)(1) standards.** Acquire Business Associate agreements with Cloud Services in use by the company. □ ScreenConnect	H	H
100	**§164.530(b) - Administrative requirements - Standard: Training and Implementation specifications: Training.** Ensure that all applicable workforce members receive training pertaining to the Breach Notification Rule's requirements for notifying individuals after a breach.	H	H
100	**§164.501 - Definitions: Marketing, §164.508(a)(3) - Authorizations for uses and disclosures - Authorization: Marketing.** Ensure that everyone who may be involved with marketing has been trained and reminded what procedures are to be followed.	H	H
97	**§164.308(A)(5)(ii)(B): Protection From Malicious Software -**	H	H

Risk Score	Recommendation	Severity	Probability
	Procedure for guarding against, detecting, and reporting malicious software. Upgrade or replace computers with operating systems that are no longer supported. □ WINOS7-2 / fe80::846b:496b:a90e:a968%10,176.16.1.115 / Windows 7 Professional □ WINOS7-1 / fe80::4168:4b42:c98d:5ad1%10,176.16.1.111 / Windows 7 Professional □ NDA1-03WP / 10.0.5.127 / CentOS Linux release 7.3.1611 (Core) □ NDA1-69NO / 10.0.5.59 / CentOS Linux release 7.3.1611 (Core)		
94	**§164.312(a)(1) Access Control - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).** Enable automatic screen lock on the specified computers. □ APPSVR01\176.16.1.14\Windows Server 2016 Standard □ DCTRL01\176.16.1.12\Windows Server 2016 Standard □ DCTRL02\176.16.1.13\Windows Server 2016 Standard □ WRKSTN-09UPSPO\176.16.1.116\Windows 10 Pro □ WRKSTN-191IJQL\176.16.1.142\Windows 10 Enterprise □ WRKSTN-4171AR0\176.16.1.124\Windows 10 Enterprise □ WRKSTN-4PF2ICP\176.16.1.100\Windows 10 Pro □ WRKSTN-534MS45\176.16.1.151\Windows 10 Enterprise □ WRKSTN-85BJGJT\176.16.1.152\Windows 10 Enterprise □ WRKSTN-BDJFFLG\176.16.1.119\Windows 10 Enterprise □ WRKSTN-F0M1O27\176.16.1.125\Windows 10 Enterprise □ WRKSTN-HN95P9Q\176.16.1.139\Windows 10 Enterprise □ WRKSTN-LIFRCFU\176.16.1.146\Windows 10 Enterprise □ WRKSTN-MJOD0L9\176.16.1.120\Windows 10 Enterprise □ WRKSTN-RB3LBP3\176.16.1.122\Windows 10 Enterprise 2015 LTSB	H	H

Risk Score	Recommendation	Severity	Probability
	□ WRKSTN-U1K3NAF\176.16.1.150\Windows 10 Enterprise □ EXCHSVR01\176.16.1.15, 169.254.48.95\Windows Server 2012 R2 Standard □ FSERV01\176.16.1.16\Windows Server 2016 Standard □ SQLSVR01\176.16.1.17\Windows Server 2012 R2 Standard □ WINOS10-1\176.16.1.102\Windows 10 Enterprise □ WINOS10-2\176.16.1.108\Windows 10 Enterprise □ WINOS10-3\176.16.1.113\Windows 10 Enterprise □ WINOS10-4\176.16.1.114\Windows 10 Enterprise □ WINOS7-1\176.16.1.111\Windows 7 Professional □ WINOS7-2\176.16.1.115\Windows 7 Professional □ WINOS8-1\176.16.1.105\Windows 8.1 Pro □ WINOS8-2\176.16.1.103\Windows 8.1 Pro □ WINOS8-3\176.16.1.107\Windows 8.1 Pro □ WINOS8-4\176.16.1.110\Windows 8.1 Pro		
94	**§164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.** Install a commercial grade anti-virus program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report. □ Computer: WS2012IT IP Address: 176.16.1.135	H	H
94	**§164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.** Install a commercial grade anti-spyware program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report. □ Computer: WS2012IT IP Address: 176.16.1.135	H	H
90	**§164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.** Ensure anti-virus programs on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report are up-to-date. □ Computer: APPSVR01 IP Address: 176.16.1.14 Security Center: Windows Defender □ Computer: WINOS7-2 IP Address: 176.16.1.115 Security Center: Windows Defender □ Computer: WINOS7-1 IP Address: 176.16.1.111 Security Center: Windows Defender	H	H

Risk Score	Recommendation	Severity	Probability
90	**§164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.** Ensure anti-spyware programs on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report are up-to-date. □ Computer: WRKSTN-F0M1O27 IP Address: 176.16.1.125 Security Center: Windows Defender □ Computer: APPSVR01 IP Address: 176.16.1.14 Security Center: Windows Defender □ Computer: WRKSTN-534MS45 IP Address: 176.16.1.151 Security Center: Windows Defender □ Computer: WRKSTN-35EGQCC IP Address: 176.16.1.104 Security Center: Windows Defender □ Computer: WRKSTN-85BJGJT IP Address: 176.16.1.152 Security Center: Windows Defender □ Computer: WINOS10-1 IP Address: 176.16.1.102 Security Center: Windows Defender □ Computer: WRKSTN-LIFRCFU IP Address: 176.16.1.146 Security Center: Windows Defender □ Computer: WRKSTN-MJOD0L9 IP Address: 176.16.1.120 Security Center: Windows Defender □ Computer: WRKSTN-BDJFFLG IP Address: 176.16.1.119 Security Center: Windows Defender	H	H
88	**§164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.** Enable IPS on firewalls or investigate putting in place a firewall with IPS capabilities.	H	H
85	**§164.310(c): Workstation security - Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.** Create a written Workstation Security Procedure and share it with the individuals responsible for its implementation.	H	H
85	**§164.308(a)(1)(ii)(C): Sanction policy - Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.** Create a written Sanction Policy and share it with your workforce members.	H	H
85	**§164.308(a)(6)(i): Security incident procedures - Implement**	H	H

Risk Score	Recommendation	Severity	Probability
	policies and procedures to address security incidents. Missing written Security Incident Response and Reporting Plan. Create a written Security Incident Response and Reporting Plan and share it with the individuals responsible for its implementation.		
85	**§164.308(a)(7)(i): Contingency plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. (ii) Implementation specifications: (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data. (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. (D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans. (E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components** Create a written Emergency Mode Operations Plan and share it with the individuals responsible for its implementation.	H	H
85	**§164.308(a)(8): Evaluation - Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.** Implement ongoing monitoring and planning to evaluate security plans and procedures to adequately protect ePHI.	H	H
85	**§164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the**	H	H

Risk Score	Recommendation	Severity	Probability
	facility. Create a written Data Backup and Storage Procedure and share it with the individuals responsible for its implementation.		
85	**§164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.** Create a written Media Reuse Policy and share it with the individuals responsible for its implementation.	H	H
85	**§164.312(c)(1): Integrity - Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.** Create a written procedure to protect the Integrity of Data Against Improper Alteration and Destruction and share it with the individuals responsible for its implementation.	H	H
85	**§164.312(e)(1): Transmission Security - Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.** Create a written procedure to protect and encrypt ePHI during transmission.	H	H
85	**§164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.** Create a written Facility Security Plan and share it with the individuals responsible for its implementation.	H	H
82	**§164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.** Create a written procedure for maintaining Facility Access Control maintenance records and share it with the individuals responsible for its implementation.	H	H

Risk Score	Recommendation	Severity	Probability
80	**§164.404 - Notification to individuals - Standard: General rule for unsecured protected health information breach notification.** Attach a copy of the Policy & Procedures Document or portion related to the Breach Individual Notification Policy.	M	H
80	**§164.512(e) - Uses and Disclosure - Standard: Disclosures for judicial and administrative proceedings.** Attach copy of Law Enforcement, Court Orders and Subpoenas Policy.	M	H
80	**§ 164.502(e) Uses and disclosures of protected health information, § 164.504(e) - Uses and disclosures - organizational requirements, § 164.532(d) - Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.** Attach copy of Business Associates Policy.	M	H
80	**§164.520 - Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.** Attach a copy of the Notice of Privacy Practices	M	H
80	**§164.510(b) - Uses and disclosures for which authorization is required - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.** Attach copy Uses & Disclosures - Emergencies & Disasters.	M	H
80	**§164.408 - Notification to the Secretary - Standard: A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2) notify the Secretary of HHS.** Attach a copy of the Policy & Procedures Document or portion related to the Breach Reporting Policy.	M	H
80	**§164.402 - Definitions - Risk assessment of breach.** Attach a copy of the Policy & Procedures Document or portion related to the Breach Risk Assessment Policy.	M	H
80	**§164.502(e) Uses and disclosures of protected health information, §164.504(e) - Uses and disclosures - organizational requirements, §164.532(d) - Transition**	M	H

Risk Score	Recommendation	Severity	Probability
	provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance. Attach copy of Minimum Necessary Access Policy.		
80	**§164.502(e) Uses and disclosures of protected health information, §164.504(e) - Uses and disclosures - organizational requirements, §164.532(d) - Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.** Attach evidence of minimum necessary access internal auditing including, records of reviews of access to paper and electronic records.	M	H
80	**§164.501 - Definitions: Marketing, §164.508(a)(3) - Authorizations for uses and disclosures - Authorization: Marketing.** Attach copy of HIPAA-related Marketing Policy.	M	H
77	**§164.308(a)(5)(ii)(d): Password Management - Procedures for creating, changing, and safeguarding passwords.** Enable account lockout for all users. □ BDRSTN01	H	H
75	**§164.308(a)(5)(ii)(d): Password Management - Procedures for creating, changing, and safeguarding passwords.** Enable enforcement of password length to more than 8 characters. □ BDRSTN01	H	M
75	**§164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.** Address patching on computers missing 1-3 security patches. □ WINOS7-2 / fe80::846b:496b:a90e:a968%10,176.16.1.115 / Windows 7 Professional	M	H
75	**§164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.** Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.	H	H

Risk Score	Recommendation	Severity	Probability
	□ Name: OpenSSH auth2-gss.c User Enumeration Vulnerability (Windows) / CVSS: 5 / IP: 97.62.96.27 □ Name: OpenSSH sftp-server Security Bypass Vulnerability (Windows) / CVSS: 5 / IP: 97.62.96.27 □ Name: OpenSSH User Enumeration Vulnerability-Aug18 (Windows) / CVSS: 5 / IP: 97.62.96.27		

Medium Risk

Risk Score	Recommendation	Severity	Probability
65	**§164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.** It is recommended to not use third-party remote access services on systems that could potentially display or access ePHI. □ ScreenConnect on Workstation WRKSTN-U1K3NAF □ ScreenConnect on Workstation WRKSTN-HN95P9Q □ ScreenConnect on Workstation WRKSTN-QFC42PE □ ScreenConnect on Workstation WRKSTN-F0M1O27 □ ScreenConnect on Workstation WRKSTN-RB3LBP3 □ ScreenConnect on Workstation APPSVR01 □ ScreenConnect on Workstation WRKSTN-534MS45 □ ScreenConnect on Workstation WINOS8-2 □ ScreenConnect on Workstation WRKSTN-35EGQCC □ ScreenConnect on Workstation WRKSTN-85BJGJT □ ScreenConnect on Workstation BDRSTN01 □ ScreenConnect on Workstation WINOS10-1 □ ScreenConnect on Workstation WINOS8-3 □ ScreenConnect on Workstation WRKSTN-LIFRCFU □ ScreenConnect on Workstation WRKSTN-09UPSPO □ ScreenConnect on Workstation WRKSTN-MJOD0L9 □ ScreenConnect on Workstation WRKSTN-191IJQL □ ScreenConnect on Workstation WINOS10-3 □ ScreenConnect on Workstation WRKSTN-4171AR0 □ ScreenConnect on Workstation WRKSTN-	M	L

Risk Score	Recommendation	Severity	Probability
	MA551PF □ ScreenConnect on Workstation WINOS10-4 □ ScreenConnect on Workstation WINOS10-2 □ ScreenConnect on Workstation EXCHSVR01 □ ScreenConnect on Workstation WINOS8-1 □ ScreenConnect on Workstation WINOS8-4 □ ScreenConnect on Workstation WS2012IT □ ScreenConnect on Workstation SQLSVR01 □ ScreenConnect on Workstation FSERV01 □ ScreenConnect on Workstation WRKSTN-4PF2ICP □ ScreenConnect on Workstation WRKSTN-BDJFFLG □ ScreenConnect on Workstation SQL02 □ ScreenConnect on Workstation WINOS7-2 □ ScreenConnect on Workstation WRKSTN-F6CKERQ □ ScreenConnect on Workstation WINOS7-1 □ ScreenConnect on Workstation DCTRL01 □ ScreenConnect on Workstation DCTRL02		

Low Risk

Risk Score	Recommendation	Severity	Probability
35	**45 CFR §164.308(A)(3) - Standard Workforce Security - Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.** Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary. □ abnetuser\A Bower □ ajnetuser\A Jones □ Administrator\Administrator □ dnetuser\D Bower □ dknetuser\D Ketterman □ dwnetuser\D White □ jsnetuser\J Smith □ jwnetuser\J Weston □ lwnetuser\L Winter □ mgnetuser\M Green □ mpnetuser\M Porter □ mwnetuser\M Wan □ pknetuser\P Kringle	L	M

Risk Score	Recommendation	Severity	Probability
	□ psnetuser\PS Admin □ sknetuser\S Kraugh □ thnetuser\T Harrison □ unetuser\unitrends admin □ wpnetuser\W Parson □ ydnetuser\Y Drew		
30	**§164.308(A)(5)(ii)(D): Password Management - Procedures for creating, changing, and safeguarding passwords.** Investigate all accounts with passwords set to never expire and configure them to expire regularly. □ Domain: coveredentity.com Username: ajadmin Displayname: A Jones □ Domain: coveredentity.com Username: dadmin Displayname: D Bower □ Domain: coveredentity.com Username: dkadmin Displayname: D Ketterman □ Domain: coveredentity.com Username: dwadmin Displayname: D White □ Domain: coveredentity.com Username: jsadmin Displayname: J Smith □ Domain: coveredentity.com Username: jwadmin Displayname: J Weston □ Domain: coveredentity.com Username: lwadmin Displayname: L Winter □ Domain: coveredentity.com Username: mgadmin Displayname: M Green □ Domain: coveredentity.com Username: mpadmin Displayname: M Porter □ Domain: coveredentity.com Username: mwadmin Displayname: M Wan □ Domain: coveredentity.com Username: mptest Displayname: MP Talman □ Domain: coveredentity.com Username: pkadmin Displayname: P Kringle □ Domain: coveredentity.com Username: psadmin Displayname: PS Admin □ Domain: coveredentity.com Username: thadmin Displayname: T Harrison □ Domain: coveredentity.com Username: uadmin Displayname: unitrends admin □ Domain: coveredentity.com Username: wpadmin Displayname: W Parson □ Domain: coveredentity.com Username: ydadmin Displayname: Y Drew	L	L
25	**§164.308(a)(3)(ii)(C): - Termination Procedures - Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in**	L	L

Risk Score	Recommendation	Severity	Probability
	a)(3)(ii)(B) of this section. Disable or remove user accounts for users that have not logged on to active directory in 90 days. □ ajnetuser \ A Jones □ arogers \ Aaron Rogers □ Administrator \ Administrator □ dwnetuser \ D White □ ebland \ Eric Bland □ jkristian \ Jabez Kristian □ jashter \ Jacob Ashter □ jgross \ Janet Gross □ jknight \ Janet Knight □ jcole \ Jerry Coleman □ jcamps \ John Camps □ jdejesus \ Jone DeJesus □ mwnetuser \ M Wan □ mjones \ Marley Jones □ mptest \ MP Talman □ pwysocki \ Pat Wysocki □ psnetuser \ PS Admin □ sjames \ Stan James □ tshields \ Tin Shields □ unetuser \ unitrends admin □ wpnetuser \ W Parson □ ydnetuser \ Y Drew		
13	**§164.308(A)(3)(ii)(C): - Termination Procedures - Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in a)(3)(ii)(B) of this section.** Disable or remove user accounts for users that have not logged on to active directory in 30 days. □ ajnetuser \ A Jones □ arogers \ Aaron Rogers □ Administrator \ Administrator □ dwnetuser \ D White □ ebland \ Eric Bland □ jkristian \ Jabez Kristian □ jashter \ Jacob Ashter □ jgross \ Janet Gross □ jknight \ Janet Knight □ jcole \ Jerry Coleman □ jcamps \ John Camps □ jdejesus \ Jone DeJesus □ mwnetuser \ M Wan □ mjones \ Marley Jones □ mptest \ MP Talman □ pwysocki \ Pat Wysocki	L	L

Risk Score	Recommendation	Severity	Probability
	□ psnetuser \ PS Admin □ sjames \ Stan James □ tshields \ Tin Shields □ unetuser \ unitrends admin □ wpnetuser \ W Parson □ ydnetuser \ Y Drew		
12	**§164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.** Ensure malware filtering subscriptions are up-to-date.	L	L
11	**§164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.** Evaluate the pros and cons of enabling object level access or ensure alternative methods for breach identification are in place. □ APPSVR01 / fe80::8838:46d8:ada5:22d8%5,176.16.1.14 / Windows Server 2016 Standard □ BDRSTN01 / fe80::3990:1477:6523:5e5%6,176.16.1.140 / Windows Server 2016 Standard □ WRKSTN-09UPSPO / fe80::987:2059:c582:6c21%6,176.16.1.116 / Windows 10 Pro □ WRKSTN-191IJQL / fe80::586d:a01c:9bb6:cebf%17,176.16.1.142 / Windows 10 Enterprise □ WRKSTN-4171AR0 / fe80::ecb4:bd94:5108:889c%6,176.16.1.124 / Windows 10 Enterprise □ WRKSTN-4PF2ICP / fe80::529:1457:17a6:d616%3,176.16.1.100 / Windows 10 Pro □ WRKSTN-534MS45 / fe80::980b:fcf8:d78a:e764%10,176.16.1.151 / Windows 10 Enterprise □ WRKSTN-85BJGJT / fe80::6545:f81b:6d3e:8abd%12,176.16.1.152 / Windows 10 Enterprise □ WRKSTN-BDJFFLG / fe80::8c50:2d27:cafa:149d%2,176.16.1.119 / Windows 10 Enterprise □ WRKSTN-F0M1O27 / fe80::465:ffab:bd25:5bd1%5,176.16.1.125 / Windows 10 Enterprise □ WRKSTN-HN95P9Q / fe80::e840:a67f:157:b2af%4,176.16.1.139 / Windows 10 Enterprise	L	L

Risk Score	Recommendation	Severity	Probability
	□ WRKSTN-LIFRCFU / fe80::45a6:ce8d:a850:a56e%3,176.16.1.146 / Windows 10 Enterprise □ WRKSTN-MJOD0L9 / fe80::f9ad:5577:5428:7f28%4,176.16.1.120 / Windows 10 Enterprise □ WRKSTN-U1K3NAF / fe80::459f:d5d3:409e:6c90%4,176.16.1.150 / Windows 10 Enterprise □ EXCHSVR01 / fe80::a427:ce0:90f0:f85b%12,fe80::c48a:8133:22db:305f%15, 176.16.1.15,169.254.48.95 / Windows Server 2012 R2 Standard □ FSERV01 / fe80::5c2b:4a84:e6ce:aca8%5,176.16.1.16 / Windows Server 2016 Standard □ SQLSVR01 / fe80::59bd:b2c6:5a41:f7b3%12,176.16.1.17 / Windows Server 2012 R2 Standard □ WINOS10-1 / fe80::6c65:7afe:58c2:6f95%10,176.16.1.102 / Windows 10 Enterprise □ WINOS10-2 / fe80::f8f9:3f5c:b6f2:1747%3,176.16.1.108 / Windows 10 Enterprise □ WINOS10-4 / fe80::29e7:e185:a561:7b15%4,176.16.1.114 / Windows 10 Enterprise □ WINOS7-1 / fe80::4168:4b42:c98d:5ad1%10,176.16.1.111 / Windows 7 Professional □ WINOS8-1 / fe80::94ce:ef7f:e97b:e4fa%3,176.16.1.105 / Windows 8.1 Pro □ WINOS8-3 / fe80::c85c:9edf:4397:9a11%3,176.16.1.107 / Windows 8.1 Pro □ WINOS8-4 / fe80::6dc8:a863:3146:ce06%3,176.16.1.110 / Windows 8.1 Pro		
1	**§164.308(a)(1)(ii)(D): Information System Activity Review - Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security tracking reports.** Evaluate the necessity of generic logins and reduce their use when possible. □ coveredentity.com \ Administrator	L	L