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.

Prepared for:
HIPAA – Covered
Entity Prepared by:

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.

High Risk

Risk Score	Recommendation	Severity	Probability
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.	H	H
90	**§164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.** Address patching on computers missing 4+ security patches. □ PABUILD / 10.0.7.60 / Windows Server 2003 □ DC01 / fe80::c479:f74:16d0:1a95%16,172.20.1.3,10.0.1.3 / Windows Server 2012 Standard □ DC02 / 172.20.0.4,10.0.1.4 / Windows Server 2012 R2 Datacenter □ DC03 / 172.20.0.23 / Windows Server 2012 R2 Datacenter □ DEV_2012-CORE / 10.0.7.53 / Hyper-V Server 2012 □ DEVTFS / 10.0.7.69 / Windows Server 2012 Standard □ DEVWIKI / 10.0.7.62 / Windows Server 2003 □ FILE2012-1 / 10.0.1.41 / Windows Server 2012 R2 Standard □ HV01 / 10.0.1.111 / Windows Server 2012 R2 Standard □ HV02 / 10.0.7.27 / Windows Server 2012 R2 Standard □ HV03 / 10.0.1.139,10.0.1.131,10.0.1.135,10.0.1.132 / Windows Server 2012 Standard □ HV04 / 10.0.1.141,10.0.1.149,10.0.1.142,10.0.1.145 / Windows Server 2012 Standard □ HV05 / 10.0.7.61 / Windows Server 2012 R2 Standard □ JAGA / 10.0.7.67 / Windows Server 2003 □ MYCO-ATL-CORE / 10.0.1.17 / Windows Server 2003 R2 □ MYCOROOTAUTH / 10.0.1.44 / Windows Server 2012 R2 Datacenter □ PSIMPSON1 / 10.0.7.32 / Windows 7 Enterprise	H	H

Risk Score	Recommendation	Severity	Probability
	□ SHAREPOINT-01 / 10.0.1.71 / Windows Server 2012 Datacenter □ SQL2012-01 / 10.0.1.61 / Windows Server 2012 R2 Datacenter □ UTIL01 / 172.20.0.5,10.0.1.5,10.0.7.89 / Windows Server 2008 R2 Datacenter □ UTIL12 / 10.0.1.15 / Windows Server 2012 R2 Standard		
89	**§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.** Create or modify the existing Business Associates Agreements to comply with the 2013 HIPAA Omnibus Final Rule.	H	H
88	**§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** Perform an analysis of application data and criticality. Use the analysis to properly implement safeguards that protect critical data.	H	H
85	**§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).** Create a written Emergency Access Procedure and share it with the individuals responsible for its implementation.	H	H

Risk Score	Recommendation	Severity	Probability
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 Data Backup and Storage Procedure 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	**§164.308(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)(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.** Create a written Access Policy and share it with the individuals responsible for its implementation.	H	H
85	**§164.308(a)(6)(i): Security incident procedures - Implement 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.	H	H
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).**	H	H

Risk Score	Recommendation	Severity	Probability
	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 Disaster Recovery 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)(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**	H	H

Risk Score	Recommendation	Severity	Probability
	plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. (D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans. (E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components §164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. Create a written Contingency Plan and share it with the individuals responsible for its implementation.		
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	**§164.312(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 for maintaining Integrity Controls used during transmissions of ePHI and share it with the individuals responsible for its implementation.	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
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.**	H	H

Risk Score	Recommendation	Severity	Probability
	Create a written Access Control and Validation Procedure and share it with the individuals responsible for its implementation.		
85	**§164.310(b): Workstation use - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.** Create a written Workstation Use Policy and share it with your workforce members.	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	**§164.310(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 Disposal Policy and share it with the individuals responsible for its implementation.	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 facility.** Create a written Media Reuse Policy and share it with the individuals responsible for its implementation.	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 facility.** Create a written Media Accountability Policy 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**	H	H

Risk Score	Recommendation	Severity	Probability
	information that is being transmitted over an electronic communications network. Create a written procedure to protect and encrypt ePHI during transmission.		
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
78	**§164.308(A)(7)(ii)(A) - Data Backup Plan - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. §164.308(A)(7)(ii)(B) - Disaster Recovery Plan - Establish (and implement as needed) procedure to restore any loss of data.** Ensure that data is properly backed up on computers with ePHI. See the Endpoint Security section of the Evidence of HIPAA Compliance for a list of computers.	H	H
75	Assess the risk of each vulnerability and remediating all external vulnerabilities as prescribed. ☐ Name: Apache Tomcat Denial Of Service Vulnerability -June15 (Linux) / CVSS: 7.8 / IP: 208.32.211.104 ☐ Name: Apache Tomcat Multiple Vulnerabilities-01 (Nov14)/ CVSS: 5.0 / IP: 208.32.211.104 ☐ Name: Apache Tomcat Security Manager Security Bypass Vulnerability -June15 (Linux) CVSS: 5.0 / IP: 208.32.211.104 ☐ Name: Apache Tomcat sort and orderBy Parameters Cross Site Scripting Vulnerabilities/ CVSS: 4.3 / IP: 208.32.211.104 ☐ Name: Check for SSL Weak Ciphers/ CVSS: 4.3 / IP: 208.32.211.104 ☐ Name: Deprecated SSLv2 and SSLv3 Protocol Detection/ CVSS: 4.3 / IP: 208.32.211.104	H	H

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**	L	M

Risk Score	Recommendation	Severity	Probability
	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.		
14	**§164.308(A)(5)(ii)(B): Protection From Malicious Software - Procedure for guarding against, detecting, and reporting malicious software.** Enable malware filtering on firewalls or investigate putting in place a firewall with malware filtering services.	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.	L	L