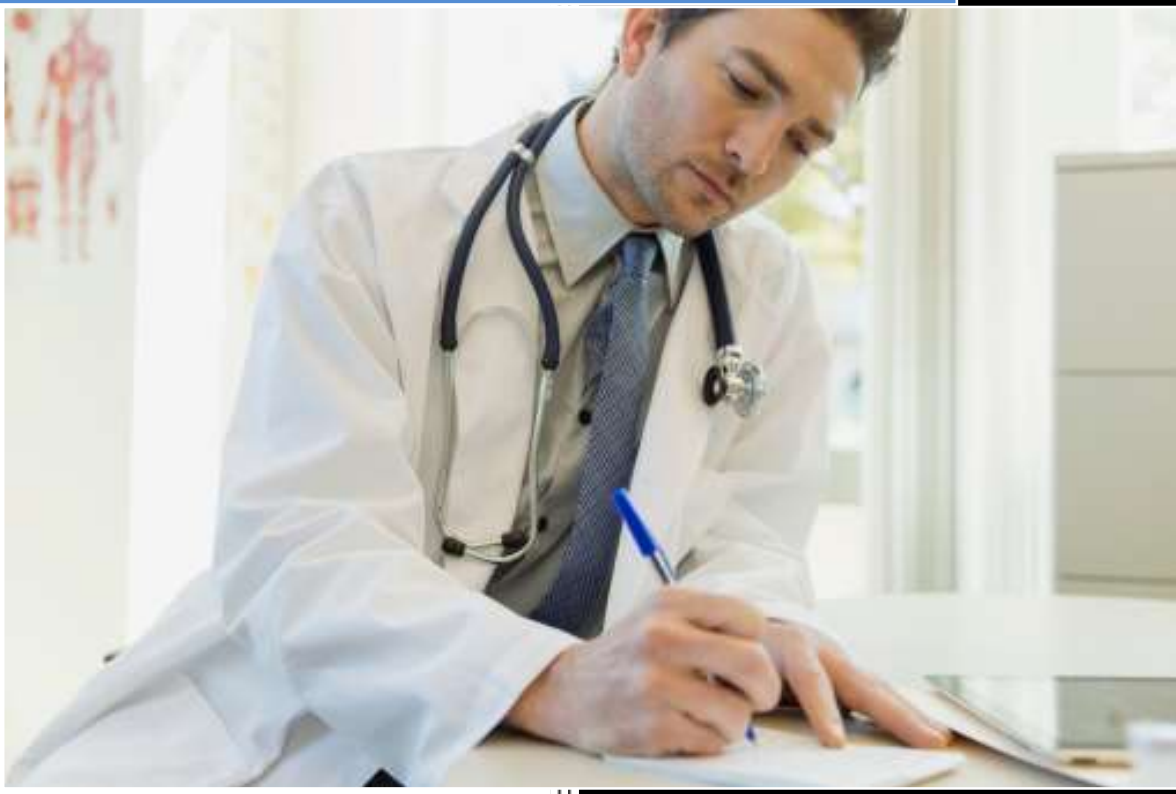
YourIT!
Your Logo Goes Here

HIPAA Assessment

HIPAA Management Plan



Scan Date: 4/1/2014

Prepared for:
Customer Name Here!
Prepared by:
Your Company Name Here!

2/26/2016

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
97	**§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.** Upgrade or replace computers with operating systems that are no longer supported. ☐ MYCOPATCH / 10.0.7.55 / Windows 2000 Server ☐ ISA1 / 10.0.1.6 / Windows Server 2003 ☐ REMOTE / 10.0.7.68 / Windows 2000 Server ☐ JAGA / 10.0.7.67 / Windows Server 2003 ☐ PABUILD / 10.0.7.60 / Windows Server 2003 ☐ DAVIS-XP / 10.0.7.10 / Windows XP Professional ☐ THRASH2 / 10.0.1.33 / Windows 2000 Server ☐ MYCO-ATL-CORE / 10.0.1.17 / Windows Server 2003 ☐ DEVWIKI / 10.0.7.62 / Windows Server 2003 ☐ MYCO30DEV / 10.0.7.65 / Windows 2000 Server	H	H
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. ☐ GENA-PC / 10.0.6.114 / Windows 8.1 Pro ☐ DEV-TEST2 / 169.254.56.1, 10.0.6.109 / Windows 8 Pro	H	H
94	**§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures 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.	H	H
94	**§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting**	H	H

Risk Score	Recommendation	Severity	Probability
	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.		
93	**§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.** Identify the necessity of using the free hosted email services and discontinue their use.	H	H
92	**§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.** Enable anti-virus program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.	H	H
92	**§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.** Enable anti-spyware program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.	H	H
90	**§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures 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.	H	H
90	**§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures 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.	H	H
88	**§164.308(a)(4): 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

Risk Score	Recommendation	Severity	Probability
85	**§164.308(a)(3) 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.** Remove access to Network Shares on systems with ePHI. ☐ DEV$ / DEV$ ☐ IUSR_DC02 / IUSR_DC02 ☐ IUSR_STEINBRENNER / IUSR_STEINBRENNER ☐ IWAM_DC02 / IWAM_DC02 ☐ IWAM_STEINBRENNER / IWAM_STEINBRENNER ☐ netvendor / netvendor ☐ SUPPORT$ / SUPPORT$ ☐ wparson / wendell	H	H
80	**§164.308(a)(4) Information Access Management - Implement policies and procedures for authorizing access to electronic protected health information.** Investigate the network shares containing ePHI with unrestricted access. Limit access to the minimum necessary. ☐ \\DC01\C$ ☐ \\INSP-TEST2\C$ ☐ \\MWEST-WIN864\C$ ☐ \\MWEST-WIN864\Share ☐ \\MWEST-WIN864\xdrive ☐ \\STORAGE01\ADMIN$ ☐ \\STORAGE01\C$ ☐ \\STORAGE01\CertEnroll ☐ \\STORAGE01\Common ☐ \\STORAGE01\D$ ☐ \\STORAGE01\ISO ☐ \\STORAGE01\OldCommon	H	H
80	**§164.308(a)(5)(ii)(d): Security Awareness and Training - Procedures for creating, changing, and safeguarding passwords.** Investigate all accounts with passwords set to never expire and configure them to expire regularly. ☐ Administrator / Administrator ☐ bvinings / Bob vinings ☐ bgelding / Beth gelding ☐ fthomas / Fred thomas	H	H

Risk Score	Recommendation	Severity	Probability
	☐ HJoel / Hank\ Joel ☐ IWAM_DC02 / IWAM_DC02 ☐ IWAM_STEINBRENNER / IWAM_STEINBRENNER ☐ JDAVIS / James DAVIS ☐ kglass / K glass ☐ kmayhem1 / k mayhem1 ☐ kjacobs / Kevin jacobs ☐ kmayhem / Kevin mayhem ☐ mparish / marcusus parish ☐ mSUMMER / Mark SUMMER ☐ mELKINS / Michael ELKINS ☐ mmayhemON / Michael mayhemON ☐ mDAVIS / michal DAVIS ☐ netvendor / netvendor ☐ pSIMPSON / Pablo SIMPSON ☐ Pkrickey / Paul krickey ☐ support / internal IT Support Team ☐ rjohnson / Ray Johnson ☐ rphillis / Rita phillis ☐ rtaylor / Rob Taylor ☐ sRammond / Sam Rammond. ☐ smurray / Sarah murray ☐ slowe / Sharlise Lowe ☐ tholmes / Tameka Holmes ☐ marcusustest / Test User ☐ thughes / Tony hughes ☐ wparson / wendell		
78	**§164.308(a)(7)(ii)(A) - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. Contingency Plan §164.308(a)(7)(ii)(b) - Establish (and implement as needed) procedures 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
77	**§164.308(a)(5)(ii)(d): Security Awareness and Training - Procedures for creating, changing, and safeguarding passwords.** Enable account lockout for all users.	H	H
75	**§164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.** Eliminate the use of unencrypted USB drives.	H	H
75	**§164.308(a)(5)(ii)(d): Security Awareness and Training -**	H	M

Risk Score	Recommendation	Severity	Probability
	Procedures for creating, changing, and safeguarding passwords. Enable enforcement of password length to 6 more characters.		
75	**§164.308(a)(5)(ii)(d): Security Awareness and Training - Procedures for creating, changing, and safeguarding passwords.** Enable password complexity to assure domain account passwords are secure.	H	H

Low Risk

Risk Score	Recommendation	Severity	Probability
50	**§164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.** Reduce or eliminate the use of USB drives in the environment.	L	H
35	**45 CFR §164.308(a)(3) - 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. ☐ byellin / Ben yellin ☐ bpratt / Bryant pratt ☐ cepps / Chris epps ☐ dbard / dennis bard ☐ eHAMMOND / Elvin HAMMOND ☐ echristy / Ethan christy ☐ fthomas / Fred thomas ☐ gHAMMOND / Greg HAMMOND ☐ HJoel / Hank\ Joel ☐ JDAVIS / James DAVIS ☐ jpane / Jim pane ☐ jcosten / Joe Costen ☐ kglass / K glass ☐ kmayhem1 / k mayhem1 ☐ kjacobs / Kevin jacobs ☐ kmayhem / Kevin mayhem ☐ TWilliams / Terry Williams	L	M

Risk Score	Recommendation	Severity	Probability
	☐ mWEST / Madeleine WEST ☐ mparish / marcusus parish ☐ mSUMMER / Mark SUMMER ☐ mELKINS / Michael ELKINS ☐ mmayhemON / Michael mayhemON ☐ pSIMPSON / Pablo SIMPSON ☐ Pkrickey / Paul krickey ☐ rphillis / Rita phillis ☐ rtaylor / Rob Taylor ☐ sRammond / Sam Rammond. ☐ sboardroom / Steve boardroom ☐ thughes / Tony hughes ☐ wparson / wendell		
30	**§164.308(a)(1)(ii)(D): Security Management Process - Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.** Enable user login auditing.	L	L
25	**§164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).** Investigate all inactive accounts and disable accounts from terminated employees and vendors. ☐ bgelding / Beth gelding ☐ bvinings / Bob vinings ☐ HJoel / Hank\ Joel ☐ hr / internal IT HR ☐ partners / internal IT Managed Services Partners ☐ info / internal IT PR ☐ prsales / internal IT Sales ☐ IUSR_STEINBRENNER / IUSR_STEINBRENNER ☐ IWAM_DC02 / IWAM_DC02 ☐ IWAM_STEINBRENNER / IWAM_STEINBRENNER ☐ jcosten / Joe Costen ☐ kglass / K glass ☐ kmayhem1 / k mayhem1 ☐ mWEST / Madeleine WEST ☐ netvendor / netvendor ☐ rtaylor / Rob Taylor ☐ smurray / Sarah murray ☐ SUPPORT$ / SUPPORT$ ☐ marcusustest / Test User	L	L

Risk Score	Recommendation	Severity	Probability
14	**§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures 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
13	**§164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).** Disable or remove user accounts for users that have not logged in in 30 days. ☐ bvinings / Bob vinings ☐ bgelding / Beth gelding ☐ HJoel / Hank\ Joel ☐ IUSR_STEINBRENNER / IUSR_STEINBRENNER ☐ IWAM_DC02 / IWAM_DC02 ☐ IWAM_STEINBRENNER / IWAM_STEINBRENNER ☐ jcosten / Joe Costen ☐ kglass / K glass ☐ kmayhem1 / k mayhem1 ☐ mWEST / Madeleine WEST ☐ netvendor / netvendor ☐ hr / internal IT HR ☐ partners / internal IT Managed Services Partners ☐ info / internal IT PR ☐ prsales / internal IT Sales ☐ rtaylor / Rob Taylor ☐ smurray / Sarah murray ☐ SUPPORT$ / SUPPORT$ ☐ marcusustest / Test User	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
1	**§164.308(a)(1)(ii)(D): Security Management Process - Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.** Evaluate the necessity of generic logins and reduce their use when possible.	L	L