HIPAA Assessment

Evidence of HIPAA Policy Compliance

Prepared for:
HIPAA - Covered Entity Prepared by:

Table of Contents

1 - Overview

Our organization has adopted written Policies & Procedures that describe in detail the tasks that we have committed to undertake to fulfill our HIPAA compliance reporting requirements.

We start by performing a periodic Risk Analysis to identify threats and vulnerabilities to ePHI and the security of our networks and systems, in general. We then create a Risk Management Plan to prioritize remediation and ensure resolution of the issues identified in the Risk Analysis.

This document supplements the Risk Analysis and Risk Management Plan and offers substantiation and verification of policy compliance by providing confirmation of timely performance of recommendations detailed in the Risk Management Plan.

Security Officer

Name of Security Officer:

Bob Smith

Contact Information for Security Officer:

555-555-5555
bobsmith@hipaa-covered-entity.com

2 - Overall Risk

2.1 - Overall Risk

We have performed a Risk Assessment as part of our routine HIPAA compliance review. See the attached HIPAA Risk Analysis and Management Plan document.

The Risk Analysis is designed to accurately and thoroughly identify vulnerabilities and threats that impact electronic Protected Health Information (ePHI). The report is then used to assess the potential risks to the confidentiality, integrity and availability of ePHI located or held at our office.

The Risk Analysis follows industry best practice standards as described by HHS, NIST, ISACA, HIMSS or AHIMA organizations and performed no less than one time a year or after successful implementation of any major system change including an office relocation, replacement of EHR system containing PHI, etc.

3 - Environment

3.1 - Facility Access Controls

§164.310(a)(1): 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.

We implement procedures that are designed to allow authorized access and deny unauthorized access, to and within facilities, to limit access to devices that can access or store ePHI.

Computers

During a physical walkthrough, we found some computers that did not have protection against theft in place.

Comments:

Data Storage Devices

During a physical walkthrough, we found some data storage devices that did not have protection against theft in place.

Comments:

Public Viewable Screens

During a physical walkthrough, we found some screens that could potentially display ePHI viewable by the public.

Comments:

Retired/Decommissioned/Failed Systems or Storage Devices

During a physical walkthrough, we found some retired/decommissioned/failed systems or storage devices.

Comments:

4 - Users

4.1 - Information System Activity Review / Unique User Identification

§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. **§164.312(a)(2)(i):** Access Control - Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.

We employ the use of Windows Authenticated users as a means for unique user identification.

As part of our regular review of system activity, we validate the list of current users and identify former employees and vendors who may still have access. This review involves looking at audit logs, access reports, and reviewing security incident tracking reports. During the review, generic accounts logins are also identified for further investigation. *See the User Identification Worksheet and Login History by Computer Report*

	# Enabled Users	# Disabled Users
Employee - ePHI authorization	3	0
Employee - no ePHI authorization	35	0
Vendor - ePHI authorization	0	0
Vendor - no ePHI authorization	1	0
Former Employee	0	0
Former Vendor	0	0
Service Account	10	0

Potential Generic Accounts found

Generic account logins were used on the following computers and should be investigated. The use of generic logins may prevent proper tracking and identification and is discouraged. There are legitimate uses for generic logins, such as limited administrative access and use, as well as access to workstations where secondary logins are required to access ePHI. If access is deemed inappropriate, further action should be taken to ensure the situation is remediated.

Generic Account	First Name	Last Name	Computer	IP Address
DEV$	DEV$			
hr	internal	HR		
info	internal	PR		
partners	internal	Partners		
prsales	internal	Sales		
support	internal	Team		

Generic Account	First Name	Last Name	Computer	IP Address
SUPPORT$	SUPPORT$			

Potential ePHI access

The following users that were marked in the User Identification Worksheet as not having access to ePHI have attempted to or logged into computer identified as having ePHI and should be investigated.*If access is deemed inappropriate, further action should be taken to ensure the situation is remediated.*

Account	First Name	Last Name	Computer	IP Address
Administrator	Administrator		BKRICKEY-WIN7	10.0.7.74
Administrator	Administrator		MWEST-WIN864	10.0.7.11
BKRICKEY	Beth	krickey	BKRICKEY-WIN7	10.0.7.74
gHAMMOND	Greg	HAMMOND	BKRICKEY-WIN7	10.0.7.74
gHAMMOND	Greg	HAMMOND	MWEST-WIN864	10.0.7.11
JDAVIS	James	DAVIS	BKRICKEY-WIN7	10.0.7.74
JDAVIS	James	DAVIS	MWEST-WIN864	10.0.7.11
kjacobs	Kevin	jacobs	MWEST-WIN864	10.0.7.11
mparish	marcusus	parish	BKRICKEY-WIN7	10.0.7.74
mparish	marcusus	parish	MWEST-WIN864	10.0.7.11
mSUMMER	Mark	SUMMER	BKRICKEY-WIN7	10.0.7.74
mSUMMER	Mark	SUMMER	MWEST-WIN864	10.0.7.11
pSIMPSON	Pablo	SIMPSON	BKRICKEY-WIN7	10.0.7.74
pSIMPSON	Pablo	SIMPSON	MWEST-WIN864	10.0.7.11
rphillis	Rita	phillis	MWEST-WIN864	10.0.7.11
sRammond	Sam	Rammond.	BKRICKEY-WIN7	10.0.7.74
sRammond	Sam	Rammond.	MWEST-WIN864	10.0.7.11
wparson	wendell		BKRICKEY-WIN7	10.0.7.74
wparson	wendell		MWEST-WIN864	10.0.7.11

4.2 - Termination Procedures

§164.308(a)(3)(ii)(c): Termination Procedures - 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).

No issues were noted. See the User Identification Worksheet and Login History by Computer Report.

4.3 - Establish Clear Job Description and Responsibilities / Access Authorization

§164.308(a)(3): 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.
§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.

The following are Network Shares that have been identified as having ePHI (see Network Share Identification Worksheet). They are listed below with their current security settings. Unrestricted shares, allowing access to everyone, are marked in **RED BOLD**. Shares that allow access by a User identified as not having access to ePHI are flagged in RED. See the Share Permission Report for a detailed listing of network shares and their settings.

Permissions for Share with ePHI

Share	ePHI	Share Type	User/Group	Share Permissions		
				Full Control	Change	Read
\\MWEST-WIN864\Share (C:\Share)	**Has ePHI**	Disk	**Everyone**	✓	✓	✓
\\MWEST-WIN864\xdrive (C:\xdrive)	**Has ePHI**	Disk	BUILTIN\Administrators	✓	✓	✓
			Everyone	✓	✓	✓
\\STORAGE01\CertEnroll (C:\Windows\system32\CertSrv\CertEnroll)	**Has ePHI**	Disk	**Everyone**			✓
			BUILTIN\Administrators	✓	✓	✓
\\STORAGE01\Common (D:\Shared Files\Common)	**Has ePHI**	Disk	**Everyone**		✓	✓
			BUILTIN\Administrators	✓	✓	✓
\\STORAGE01\ISO (E:\Shared Folders\ISO)	**Has ePHI**	Disk	BUILTIN\Administrators	✓	✓	✓
			Everyone	✓	✓	✓
\\STORAGE01\OldCommon (E:\OldCommon)	**Has ePHI**	Disk	BUILTIN\Administrators	✓	✓	✓
			Everyone	✓	✓	✓

File System Permissions for Share with ePHI

Share	Share Type	User/Group	File System Permissions	Type

Share	Share Type	User/Group	File System Permissions	Type
\\DC01\C$ (C:\)	Special	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	AppendData	Allow
		BUILTIN\Users	CreateFiles	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\INSP-TEST2\C$ (C:\)	Special	NT AUTHORITY\Authenticated Users	AppendData	Allow
		NT AUTHORITY\Authenticated Users	Special (-536805376)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\MWEST-WIN864\C$ (C:\)	Special	NT AUTHORITY\Authenticated Users	AppendData	Allow
		NT AUTHORITY\Authenticated Users	Special (-536805376)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\MWEST-WIN864\Share (C:\Share)	Disk	BUILTIN\Administrators	FullControl	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT AUTHORITY\Authenticated Users	Modify, Synchronize	Allow
		NT AUTHORITY\Authenticated Users	Special (-536805376)	Allow
\\MWEST-WIN864\xdrive (C:\xdrive)	Disk	NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		PIT\mWEST	FullControl	Allow
		PIT\rphillis	FullControl	Allow
\\STORAGE01\ADMIN$ (C:\Windows)	Special	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	Modify, Synchronize	Allow
		BUILTIN\Administrators	Special (268435456)	Allow
		BUILTIN\Administrators	Modify, Synchronize	Allow

Share	Share Type	User/Group	File System Permissions	Type
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
\\STORAGE01\C$ (C:\)	Special	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	AppendData	Allow
		BUILTIN\Users	CreateFiles	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\STORAGE01\CertEnroll (C:\Windows\system32\CertSrv\CertEnroll)	Disk	NT SERVICE\TrustedInstaller	FullControl	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Administrators	Special (268435456)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		BUILTIN\Users	Special (-1610612736)	Allow
		CREATOR OWNER	Special (268435456)	Allow
\\STORAGE01\Common (D:\Shared Files\Common)	Disk	CREATOR OWNER	FullControl	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		PIT\Domain Admins	FullControl	Allow
		PIT\Domain Users	FullControl	Allow
		PIT\sboardroom	FullControl	Allow
		PIT\RLindy	FullControl	Allow
		PIT\dHAROLD	FullControl	Allow
		PIT\kjames	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		PIT\Domain Admins	FullControl	Allow
		CREATOR OWNER	FullControl	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Users	CreateFiles, Synchronize	Allow
		BUILTIN\Users	AppendData, Synchronize	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow

Share	Share Type	User/Group	File System Permissions	Type
\\STORAGE01\D$ (D:\)	Special	Everyone	ReadAndExecute, Synchronize	Allow
		CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	AppendData	Allow
		BUILTIN\Users	CreateFiles	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\STORAGE01\ISO (E:\Shared Folders\ISO)	Disk	Everyone	ReadAndExecute, Synchronize	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		PIT\Pkrickey	FullControl	Allow
\\STORAGE01\OldCommon (E:\OldCommon)	Disk	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		BUILTIN\Users	CreateFiles, AppendData	Allow

4.4 - Evaluate Existing Security Measures Related to Access Controls

§164.308(a)(4): Information Access Management - Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

A policy and procedure for authorizing access to ePHI is currently not available.

§164.308(a)(5)(i): Security Awareness And Training - Implement a security awareness and training program for all members of its workforce (including management).

Our employees have not yet received training on how to avoid becoming a victim of technology threats.

4.5 - Administrator Review

§164.308(a)(4): Information Access Management - Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

Domain Administrators and Administrators in general tend to have a higher level of access than other user and should be clearly identified. The following is a list of all users with administrative roles in regards to the network environment.

Domain: Corp.MyCo.com

Username	Name	Member Of
byellin	Ben yellin	**Administrators** Builtin **DHCP Administrators** **Domain Admins** Users
bpratt	Bryant pratt	**Administrators** Builtin **Domain Admins** Remote Desktop Users Users
cepps	Chris epps	**Administrators** Builtin **Domain Admins** Users
dbard	dennis bard	**Domain Admins** **Enterprise Admins** **Schema Admins** Users
eHAMMOND	Elvin HAMMOND	**Domain Admins** Users
echristy	Ethan christy	Builtin **Domain Admins** PIT Support Team Remote Desktop Users Users
fthomas	Fred thomas	**Domain Admins** Executive Users
gHAMMOND	Greg HAMMOND	**Domain Admins** Users
HJoel	Hank\ Joel	**Administrators** Builtin **DHCP Administrators** **Domain Admins** PIT Support Team Users
JDAVIS	James DAVIS	**AppV Administrators** Appv Users

Username	Name	Member Of
		Builtin **Domain Admins** **Enterprise Admins** PIT Support Team Remote Desktop Users Users
jpane	Jim pane	**Administrators** Builtin **Domain Admins** Remote Desktop Users Users
jcosten	Joe Costen	**AppV Administrators** Appv Users **Domain Admins** PIT Support Team Users
kglass	K glass	**Domain Admins** Users
kmayhem1	k mayhem1	**Administrators** Builtin **Domain Admins** Executive Users
kjacobs	Kevin jacobs	**Domain Admins** Users
kmayhem	Kevin mayhem	**Administrators** Builtin **Domain Admins** Executive Users
TWilliams	Terry Williams	**Domain Admins** Users
mWEST	Madeleine WEST	**Domain Admins** PIT Support Team Users
mparish	marcusus parish	**Domain Admins** Users
mSUMMER	Mark SUMMER	**Administrators** Builtin **Domain Admins** Users
mELKINS	Michael ELKINS	**Domain Admins** Users
mmayhemON	Michael mayhemON	**Administrators** Builtin **Domain Admins** Executive Users
pSIMPSON	Pablo SIMPSON	**Administrators** Builtin **Domain Admins** PIT Support Team Users

Username	Name	Member Of
Pkrickey	Paul krickey	**Domain Admins** **Enterprise Admins** PIT Support Team **Schema Admins** Users
rphillis	Rita phillis	**Domain Admins** **Exchange Organization Administrators** Users
rtaylor	Rob Taylor	Builtin **Domain Admins** Remote Desktop Users Users
sRammond	Sam Rammond.	**Administrators** Builtin **Domain Admins** PIT Support Team Users
sboardroom	Steve boardroom	**Administrators** Builtin **Domain Admins** Group Policy Creator Owners **Schema Admins** Users
thughes	Tony hughes	**Domain Admins** **Exchange Organization Administrators** Users
wparson	wendell	**Domain Admins** Executive Users

4.6 - Password Management

§164.308(a)(5)(ii)(b): Implementation Specifications: Password Management - Procedures for creating, changing, and safeguarding passwords.

Proper password management is vital for ensuring the security of the network. Password complexity and expiration policy should be enabled and enforced by Group Policy when possible.

Policy	Setting	Computers
Password Policy Consistency	Consistent	
Enforce password history	0 passwords remembered	All Sampled
Maximum password age	42 days	All Sampled
Minimum password age	0 days	All Sampled
Minimum password length	0 characters	All Sampled
Password must meet complexity requirements	Disabled	All Sampled
Store passwords using reversible encryption	Disabled	All Sampled

Proper account lockout policy settings will prevent both interactive and automated attempts to compromise passwords.

Policy	Setting	Computers
Account Lockout Policy Consistency	Consistent	
Account lockout duration	Not Applicable	All Sampled
Account lockout threshold	0 invalid logon attempts	All Sampled
Reset account lockout counter after	Not Applicable	All Sampled

Except for service accounts, all passwords for users that can potentially log in should be set to expire on a regular basis. The following users have passwords that are set to never expire:

Corp.MyCo.com

Administrator, bgelding, BKRICKEY, fthomas, HJoel, JDAVIS, kglass, kjacobs, kmayhem, kmayhem1, marcusustest, mDAVIS, mELKINS, mmayhemON, mparish, mSUMMER, netvendor, Pkrickey, pSIMPSON, rjohnson, rphillis, rtaylor, slowe, smurray, sRammond, support, tholmes, thughes, wparson

Local Account Password Analysis

This section contains the password strength analysis using MBSA to determine risk. Systems with security risks are highlighted in red.

IP Range for MBSA scan: 10.0.7.0-10.0.7.255

IP Address	Computer Name	Assessment
10.0.7.10	PIT\OPS001	Strong Security

IP Address	Computer Name	Assessment
		Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.11	PIT\MWEST-WIN864	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.18	PIT\PSIMPSON-WIN764	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.19	PIT\SLOWE-WIN7	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.20	PIT\SE-DAVIS	Strong Security Administrator - Disabled Guest - Weak, Disabled
10.0.7.26	PIT\MELKINS-HP	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.27	PIT\HV02	Strong Security Guest - Weak, Disabled
10.0.7.28	PIT\TANDEM	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.29	PIT\MARKETING-1	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.31	PIT\MmayhemON1	Strong Security Guest - Weak, Disabled
10.0.7.32	PIT\PSIMPSON1	Potential Risk Administrator - Weak, Disabled Guest - Weak, Disabled pablo - Does not meet account policy
10.0.7.43	PIT\ISA1	Strong Security Guest - Weak, Disabled SUPPORT_388945a0 - Disabled
10.0.7.44	PIT\JIM-WIN8	Strong Security Administrator - Disabled Guest - Weak, Disabled
10.0.7.47	PIT\REX	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.53	PIT\DEV_2012-CORE	Strong Security Guest - Weak, Disabled
10.0.7.54	PIT\PKWIN8	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.57	PIT\RANCOR	Strong Security Guest - Disabled
10.0.7.60	PIT\PABUILD	Strong Security Guest - Weak, Disabled SUPPORT_388945a0 - Disabled
10.0.7.61	PIT\HV05	Strong Security

IP Address	Computer Name	Assessment
		Guest - Weak, Disabled
10.0.7.62	PIT\DEVWIKI	Strong Security Guest - Weak, Disabled SUPPORT_388945a0 - Disabled
10.0.7.63	PIT\JIM-WIN7	Potential Risk Administrator - Weak, Disabled Guest - Weak, Disabled jim - Does not meet account policy
10.0.7.65	PIT\MYCO30DEV	Potential Risk Guest - Weak, Disabled TsInternetUser - Access denied.
10.0.7.67	PIT\JAGA	Strong Security Guest - Weak, Disabled SUPPORT_388945a0 - Disabled
10.0.7.69	PIT\DEVTFS	Strong Security Guest - Weak, Disabled
10.0.7.74	PIT\BKRICKEY-WIN7	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.75	PIT\DEVWIKI	Strong Security Guest - Weak, Disabled SUPPORT_388945a0 - Disabled
10.0.7.82	PIT\PSIMPSON-WIN7TEST	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.90	PIT\JOES-PC	Strong Security Administrator - Weak, Disabled Guest - Weak, Disabled
10.0.7.100	PIT\PABUILD	Strong Security Guest - Weak, Disabled SUPPORT_388945a0 - Disabled

4.7 - Administrative Access Control

§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).

Automatic log off or lockout is required to be set on all computers. Lockout time should always be less than 15 minutes. In some circumstances, such as nearly publicly accessible or viewable computers, lockout time should be minimized as much as feasible.

Lockout Time (minutes)	# Computers	Computers
<= 5	0	
<= 10	0	
<= 15	0	
>15	0	
Not Enabled	2	GENAVE-PC, INSP-TEST2

4.8 - Audit Controls

§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.

The following are the current Windows auditing configuration:

Policy	Setting	Computers
Audit account logon events	No auditing	All Sampled
Audit account management	No auditing	All Sampled
Audit directory service access	No auditing	All Sampled
Audit logon events	**No auditing**	**All Sampled**
Audit object access	No auditing	All Sampled
Audit policy change	No auditing	All Sampled
Audit privilege use	No auditing	All Sampled
Audit process tracking	No auditing	All Sampled
Audit system events	No auditing	All Sampled

4.9 - Person or Entity Authentication

§164.312(d): Person or Entity Authentication - Weigh the relative advantages and disadvantages of commonly used authentication approaches. There are four commonly used authentication approaches available: Something a person knows, such as a password. Something a person has or is in possession of, such as a token (smart card, ATM card, etc.). Some type of biometric identification a person provides, such as a fingerprint. A combination of two or more of the above approaches.

The use of various authentication mechanisms has both advantages and disadvantages. Use of at least one of the means of ensuring a secure authentication mechanism should be in place. A combination of multiple approaches may be desirable for increased security.

Password complexity required	No
Token-based Authentication	No
Biometric Authentication	Some

5 - Servers and Local Computers

5.1 - Protection from Malicious Software

§164.308(a)(5)(ii)(b): Protection from Malicious Software - Procedures for guarding against, detecting, and reporting malicious software.

Endpoint Security Summary

This section contains a listing of detected Antivirus, Antispyware, Firewall, and Backup information as detected through *Security Center* and/or *Installed Services* for major vendors. This list is categorized by domain membership.

The \"Name\" column contains either the name of the product, None indicating the machine returned information but no product was found, or <empty> indicating information was not obtainable. Further, a status of ✓ indicates \"yes\", ×Assessment

CORP.MYCO.COM

Computer Name	Anti-virus			Anti-spyware			Firewall		Backup	
	Name	On	Current	Name	On	Current	Name	On	Name	Current
BKRICKEY-WIN7	GFI Languard	✓		GFI Languard	✓		GFI Software VIPRE	×	None	
	GFI Software VIPRE	✓	×	GFI Software VIPRE	✓	×	Windows Firewall	✓		
				Windows Defender	×	✓				
DAVIS-XP	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DC01	None			None			Windows Firewall	×	None	
DC02	None			None			Windows Firewall	✓	None	
DC03	None			None			Windows Firewall	✓	None	
DEV_2012-CORE	None			None			Windows Firewall	✓	None	
DEVTFS	None			None			Windows	×	None	

Computer Name	Anti-virus			Anti-spyware			Firewall		Backup	
	Name	On	Current	Name	On	Current	Name	On	Name	Current
							Firewall			
DEVWIKI	None			None			Windows Firewall	×	Backup Exec	✓
DHAROLD-PC										
EHAMMOND-WIN7										
EPTOWER										
FILE2012-1	None			None			Windows Firewall	✓	None	
FT-LENOVO										
GENAVE-PC	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
GHAMMOND-LT										
HV01	None			None			Windows Firewall	✓	None	
HV02	None			None			Windows Firewall	×	None	
HV03	None			None			Windows Firewall	×	None	
HV04	None			None			Windows Firewall	×	None	
HV05	None			None			Windows Firewall	✓	None	
INSP-TEST2	Windows Defender	✓	×	Windows Defender	✓	×	Windows Firewall	✓	None	
ISA1										
JAGA	None			None			Windows Firewall	×	None	
JIM-WIN7	None			Windows Defender	✓	×	Windows Firewall	✓	None	
JIM-WIN8	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
JOES-PC	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
MARKETING-1	None				✓	✓		✓	None	

Computer Name	Anti-virus			Anti-spyware			Firewall		Backup	
	Name	On	Current	Name	On	Current	Name	On	Name	Current
				Windows Defender			Windows Firewall			
MELKINS-HP	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
MmayhemON1	None			Windows Defender	×	✓	None		None	
MmayhemON-HP										
MSUMMER-LT										
MWEST-WIN864	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
MYCO30DEV	Symantec AntiVirus	✓		Symantec AntiVirus	✓		None		None	
MYCO-ATL-CORE	None			None			Windows Firewall	×	None	
MYCOPATCH										
MYCOROOTAUTH	None			None			Windows Firewall	×	None	
OPS001	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
PABUILD	None			None			Windows Firewall	×	None	
PKWin8	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
PSIMPSON1	None			None			Windows Firewall	×	None	
PSIMPSON-WIN764	Windows Defender	×	✓	Windows Defender	×	✓	Windows Firewall	✓	None	
PSIMPSON-WIN7TEST	None			Windows Defender	✓	✓	Windows Firewall	✓	None	
RANCOR	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	×	None	
REMOTE										
REX	Microsoft Security	✓	✓	Microsoft Security	✓	✓	Windows Firewall	×	None	

Computer Name	Anti-virus			Anti-spyware			Firewall		Backup	
	Name	On	Current	Name	On	Current	Name	On	Name	Current
	Essentials			Essentials						
				Windows Defender	×	✓				
SE-DAVIS	None			Windows Defender	×	✓	Windows Firewall	✓	ShadowProtect	✓
									StorageCraft	×
SHAREPOINT-01	None			None			Windows Firewall	✓	None	
SLOWE-WIN8	GFI Languard	✓		GFI Languard	✓		GFI Software VIPRE	×	None	
	GFI Software VIPRE	✓	×	GFI Software VIPRE	✓	×	Windows Firewall	✓		
	Windows Defender	×	✓	Windows Defender	×	✓				
SPIELÖÄÜ	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
SQL2012-01	None			None			Windows Firewall	✓	None	
STORAGE01	VIPRE	✓		VIPRE	✓		Windows Firewall	×	None	
TANDEM	None			Windows Defender	✓	×	Windows Firewall	✓	None	
THRASH2										
USER-PC23										
UTIL01	None			None			Windows Firewall	×	None	
UTIL12	None			None			Windows Firewall	✓	None	

No Domain

Computer Name	Anti-virus			Anti-spyware			Firewall		Backup	
	Name	On	Current	Name	On	Current	Name	On	Name	Current

Computer Name	Anti-virus			Anti-spyware			Firewall		Backup	
	Name	On	Current	Name	On	Current	Name	On	Name	Current
slowe-win7.corp.MyCo.com	None			Windows Defender	✓	✓	Windows Firewall	✓	None	

Endpoint Security Assessment

Automated detection was unable to be completed on 111 computers. The computers should be investigated to assure proper anti-virus and anti-spyware detection.

28 computers were detected as having no anti-virus or anti-spyware.

5 computers with active but out of date anti-virus or anti-spyware.

Security Patch Summary

This section contains the patching status of computers using Windows Updates and, where supported, MBSA to determine need. Computers with missing patches are highlighted in red.

IP Address	Computer Name	Issue	Score	Assessment
10.0.7.10	PIT\OPS001	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.11	PIT\MWEST-WIN864	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.18	PIT\PSIMPSON-WIN764	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.19	PIT\SLOWE-WIN7	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.20	PIT\SE-DAVIS	Developer Tools, Runtimes, and Redistributables Security Updates	Passed	No security updates are missing.
		Microsoft Application Virtualization Security Updates	Passed	No security updates are missing.
		Microsoft Lync Server and Microsoft Lync Security Updates	Passed	No security updates are missing.
		Office Communications Server And Office Communicator Security Updates	Passed	No security updates are missing.

IP Address	Computer Name	Issue	Score	Assessment
		Office Security Updates	Passed	No security updates are missing.
		Silverlight Security Updates	Passed	No security updates are missing.
		Skype Security Updates	Passed	No security updates are missing.
		SQL Server Security Updates	Passed	No security updates are missing.
		Windows Security Updates	Passed	No security updates are missing.
10.0.7.26	PIT\MELKINS-HP	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.27	**PIT\HV02**	SQL Server Security Updates	Passed	No security updates are missing.
		Windows Security Updates	**Failed (critical)**	**9 security updates are missing. 2 service packs or update rollups are missing.**
10.0.7.28	PIT\TANDEM	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.29	PIT\MARKETING-1	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.31	**PIT\MmayhemON1**	Bing Security Updates	Passed	No security updates are missing.
		Developer Tools, Runtimes, and Redistributables Security Updates	**Failed (critical)**	**1 security updates are missing.**
		Microsoft Lync Server and Microsoft Lync Security Updates	**Failed (critical)**	**1 security updates are missing. 1 service packs or update rollups are missing.**
		Office Communications Server And Office Communicator Security Updates	Passed	No security updates are missing.
		Office Security Updates	**Failed (critical)**	**15 security updates are missing.**
		Silverlight Security Updates	**Failed (critical)**	**1 security updates are missing.**
		SQL Server Security Updates	Passed	No security updates are missing.
		Windows Security Updates	**Failed (critical)**	**67 security updates are missing. 2 service packs or update rollups are**

IP Address	Computer Name	Issue	Score	Assessment
				missing.
10.0.7.32	PIT\PSIMPSON1	Developer Tools, Runtimes, and Redistributables Security Updates	Passed	No security updates are missing.
		Office Security Updates	Passed	No security updates are missing.
		SDK Components Security Updates	Passed	No security updates are missing.
		Silverlight Security Updates	Passed	No security updates are missing.
		SQL Server Security Updates	Passed	No security updates are missing.
		Windows Security Updates	Passed	No security updates are missing.
10.0.7.43	**PIT\ISA1**	**Internet Security and Acceleration Server Security Updates**	**Failed (critical)**	**1 security updates are missing. 1 service packs or update rollups are missing.**
		SQL Server Security Updates	**Failed (critical)**	**1 security updates are missing.**
		Windows Security Updates	**Failed (critical)**	**15 security updates are missing. 2 service packs or update rollups are missing.**
10.0.7.44	PIT\JIM-WIN8	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.47	**PIT\REX**	**Developer Tools, Runtimes, and Redistributables Security Updates**	**Failed (critical)**	**3 security updates are missing.**
		Microsoft Lync Server and Microsoft Lync Security Updates	**Failed (critical)**	**1 security updates are missing. 1 service packs or update rollups are missing.**
		Office Communications Server And Office Communicator Security Updates	Passed	No security updates are missing.
		Office Security Updates	**Failed (critical)**	**32 security updates are missing. 2 service packs or update rollups are missing.**
		SDK Components Security Updates	Passed	No security updates are missing.
		Silverlight Security Updates	**Failed (critical)**	**1 security updates are missing.**
		SQL Server Security Updates	Failed (non-critical)	1 service packs or update rollups are missing.

IP Address	Computer Name	Issue	Score	Assessment
		Windows Security Updates	**Failed (critical)**	**69 security updates are missing. 4 service packs or update rollups are missing.**
10.0.7.57	PIT\RANCOR	Developer Tools, Runtimes, and Redistributables Security Updates	Passed	No security updates are missing.
		Office Security Updates	Passed	No security updates are missing.
		SDK Components Security Updates	Passed	No security updates are missing.
		Silverlight Security Updates	Passed	No security updates are missing.
		SQL Server Security Updates	Passed	No security updates are missing.
		Windows Security Updates	Passed	No security updates are missing.
10.0.7.60	PIT\PABUILD	Security Updates	Unable to scan	Computer has an older version of the client and security database demands a newer version. Current version is N/A and minimum required version is N/A.
10.0.7.62	**PIT\DEVWIKI**	**Windows Security Updates**	**Failed (critical)**	**130 security updates are missing. 5 service packs or update rollups are missing.**
10.0.7.63	PIT\JIM-WIN7	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.65	PIT\MYCO30DEV	Security Updates	Unable to scan	Cannot load security CAB file.
10.0.7.67	PIT\JAGA	Security Updates	Unable to scan	Cannot load security CAB file.
10.0.7.74	PIT\BKRICKEY-WIN7	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.75	**PIT\DEVWIKI**	**Windows Security Updates**	**Failed (critical)**	**130 security updates are missing. 5 service packs or update rollups are missing.**
10.0.7.82	PIT\PSIMPSON-WIN7TEST	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.
10.0.7.90	PIT\JOES-PC	Security Updates	Unable to scan	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.

Security Patch Assessment

Automated detection was unable to be completed on 15 computers. The computers should be investigated to assure the latest patches have been applied.

Critical security patches are missing on 6 computers. These patches should be applied as soon as possible to prevent or restrict the spread of malicious software.

5.2 - Application and Data Criticality Analysis

§164.308(a)(7)(ii)(e): Application and Data Criticality Analysis - Assess the relative criticality of specific applications and data in support of other contingency plan components.

The following is an analysis of the environment looking for other areas where PHI may be found in order to identify the associated risks.

Local EHR System

Our company hosts its own EHR system locally.

We have examined the physical security and have confirmed the server is properly secured.

6 - Firewall

6.1 - Access Authorization

§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.

We employ an external firewall to prevent external attacks.

Models:

The external firewall does not have an Intrusion Prevention System. The firewall may not be a commercial grade firewall and should be upgraded.

6.2 - Protection from Malicious Software

§164.308(a)(5)(ii)(b): Procedures for guarding against, detecting, and reporting malicious software.

The external firewall does not have Malware Filtering. The firewall may not be a commercial grade firewall and should be upgraded.

6.3 - External Vulnerability Scan

§164.308(a)(5)(ii)(b): Procedures for guarding against, detecting, and reporting malicious software.

As part of our routine procedure to ensure protection from external threats, we have conducted an external vulnerability scan. The following external IP addresses were scanned and accessed:

Host Summary

Host	Analysis	Open Ports	High	Med	Low	False	CVSS
208.32.211.104	**High risk**	2	**1**	9	1	0	50.5
Total: 1	**High risk**	2	**1**	**9**	1	0	50.5

The following high and medium issues were detected. In some cases, further investigation was performed and the risk was deemed a non-issue or false positive.

208.32.211.104 ()

High (CVSS: 7.8)
NVT: Apache Tomcat Denial Of Service Vulnerability -June15 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.805704)

443

This host is installed with Apache Tomcat and is prone to denial of service vulnerability.

Medium (CVSS: 5)
NVT: Apache Tomcat Multiple Vulnerabilities-01 (Nov14) (OID: 1.3.6.1.4.1.25623.1.0.805018)

443

This host is running Apache Tomcat and is prone to multiple vulnerabilities.

Medium (CVSS: 5)
NVT: Apache Tomcat SecurityManager Security Bypass Vulnerability - June15 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.805701)

443

This host is installed with Apache Tomcat and is prone to security bypass vulnerability.

Medium (CVSS: 4.3)
NVT: Apache Tomcat sort and orderBy Parameters Cross Site Scripting Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.103032)

443

Apache Tomcat is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.

Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

443

This routine search for weak SSL ciphers offered by a service.

Medium (CVSS: 4.3)
NVT: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

443

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Medium (CVSS: 4.3)
NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087)

443

This host is installed with OpenSSL and is prone to information disclosure vulnerability.

Medium (CVSS: 4.3)
NVT: Apache Tomcat XML External Entity Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.805019)

443

This host is running Apache Tomcat and is prone to information disclosure vulnerability.

Medium (CVSS: 4.3)
NVT: OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK) (OID: 1.3.6.1.4.1.25623.1.0.805142)

443

This host is installed with OpenSSL and is prone to man in the middle attack.

Medium (CVSS: 4.3)
NVT: OpenSSL TLS DHE_EXPORT LogJam Man in the Middle Security

443

Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.805188)

This host is installed with OpenSSL and is prone to man in the middle attack.

7 - Email

7.1 - Applications and Data Criticality Analysis

§164.308(a)(7)(ii)(e): Assess the relative criticality of specific applications and data in support of other contingency plan components.

Email is stored locally on the following computers that were marked as not having ePHI:

Computer	Mailbox Files	Verified No ePHI sent through Email Account
TANDEM	sherweb 2010 03 10.pst	
GENAVE-PC	gdaniel@rapidfiretools.com.ost	

8 - Wireless

8.1 - Access Authorization

§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.

The following wireless access points were detected. Highlighted entries are SSID published by our company. We discourage the use of all non-company wireless access points.

SSID	Secured	Security	Risk Level
<blank>	Yes	RSNA_PSK	Low
Cafe1117-Guest	**No**	**IEEE80211_Open**	**High**
CBCI-697F-2.4	Yes	RSNA_PSK	Low
CSIPRESLEFT	Yes	RSNA_PSK	Low
execue	Yes	RSNA_PSK	Low
HPC4995C	**No**	**IEEE80211_Open**	**High**
HP-Print-95-Officejet Pro 8600	**No**	**IEEE80211_Open**	**High**
MBA Training	Yes	RSNA_PSK	Low
PerfIT-G	Yes	RSNA_PSK	Low
PerfIT-Guest	Yes	RSNA_PSK	Low
PIT-Domain	Yes	RSNA	Low
RKCPA	Yes	RSNA_PSK	Low
Stonehill	Yes	RSNA_PSK	Low
Stonehill2	Yes	RSNA_PSK	Low
xfinitywifi*	**No**	**IEEE80211_Open**	**High**

* See Security Exception Worksheet

Guest Wireless

We do offer guest wireless to visitors or patients.

Guest wireless is not on the same network as ePHI.

8.2 - Access Establishment & Modification

§164.308(a)(4)(ii)(c): Implement policies and procedures that, based upon the entity's access

authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

The time the wireless keys were last changed was not noted.

8.3 - Workforce Security

§164.308(a)(3)(ii)(c): Implementation Specifications: Termination Procedures - 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).

9 - Business Associates

9.1 - Service Providers

9.2 - Cloud Servers and Data Centers

§164.308(a)(7)(ii)(a): Implementation Specifications: 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) - Establish (and implement as needed) procedures to restore any loss of data.

Cloud Servers

We host computers at an external hosted facility/data center that could possibly contain ePHI.

Contact Information:	*None provided.*

Data Center

We do not have a Business Associate Agreement with the Data Center.

9.3 - Cloud Services

The following are identified Cloud Services that could potentially expose ePHI either visually or through data transmission.

Service	Computer	Explanation of Use	ePHI Risk	BA Agreement
LogMeIn	MWEST-WIN864		Yes	
LogMeIn	PSIMPSON1		No	
LogMeIn	PSIMPSON-WIN764		No	
LogMeIn	REX		No	
LogMeIn	TANDEM		No	
ScreenConnect	BKRICKEY-WIN7		Yes	
ScreenConnect	DC01		No	
ScreenConnect	GENAVE-PC		No	
ScreenConnect	HV01		No	
ScreenConnect	HV02		No	
ScreenConnect	HV03		No	
ScreenConnect	HV04		No	
ScreenConnect	HV05		No	
ScreenConnect	INSP-TEST2		Yes	
ScreenConnect	JAGA		No	
ScreenConnect	REX		No	

Service	Computer	Explanation of Use	ePHI Risk	BA Agreement
ScreenConnect	STORAGE01		No	
ScreenConnect	UTIL01		No	
TeamViewer	MARKETING-1		No	
TeamViewer	PSIMPSON1		No	
TeamViewer	PSIMPSON-WIN764		No	
TeamViewer	RANCOR		No	
TeamViewer	SE-DAVIS		No	
TeamViewer	slowe-win7.corp.MyCo.com		No	
TeamViewer	TANDEM		No	

Remote Access Cloud Services are in use and may pose potential ePHI risk. It is recommended to not use third-party remote access services on systems that could potentially display or access ePHI.

9.4 - Business Associate Agreements for Sync folders (DropBox, Box, Google Drive, etc.)

§164.308(b)(1): Business Associate Agreements 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.

No sync folder services were detected in use.