# YourIT!
## Your Logo Goes Here

# HIPAA Assessment

## Evidence of HIPAA Policy Compliance

Prepared by:
YourIT! Company, Inc.
Prepared for:
Customer Name Here!
4/2/2014

## 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:*   Joe Secoff

*Contact Information for Security Officer:*
555 Hipaa Way
Hitech, CA 90022

## 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 Assessment 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

45 CFR §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 alLOWd."

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: Reception computer is not in a secure location. Patients can walk around and easily access the computer.**

*Data Storage Devices*

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

**Comments: Flash drives lying on desks.**

*Public Viewable Screens*

**During a physical walkthrough, we did not find any screens that could potentially display ePHI viewable by the public.**

*Public Viewable Screens*

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

**Comments: Dead computers on ground.**

## 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.

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

As part 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*, *User Behavior Analysis*, *and* *Login History by Computer Report*

|  | # Enabled Users | # Disabled Users |
|---|---|---|
| Employee - ePHI authorization | 1 | 0 |
| Employee - no ePHI authorization | 47 | 30 |
| Vendor - ePHI authorization | 1 | 0 |
| Vendor - no ePHI authorization | 0 | 0 |
| **Former Employee** | **3** | 0 |
| **Former Vendor** | **1** | 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 login, 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 |
|---|---|---|---|---|
| *Administrator* | *Administrator* |  |  |  |
| *ASPNET* | *ASPNET* |  |  |  |
| *DEV$* | *DEV$* |  |  |  |
| *Guest* | *Guest* |  |  |  |
| *IUSR_DC02* | *IUSR_DC02* |  |  |  |
| *IUSR_STEINBRENNER* | *IUSR_STEINBRENNER* |  |  |  |
| *IWAM_DC02* | *IWAM_DC02* |  |  |  |
| *IWAM_STEINBRENNER* | *IWAM_STEINBRENNER* |  |  |  |
| *netvendor* | *NETVENDOR* |  |  |  |
| *SUPPORT$* | *SUPPORT$* |  |  |  |
| *SUPPORT_388945a0* | *SUPPORT_388945a0* |  |  |  |
| *TestV* | *TestV* |  |  |  |

**4.2 - Termination Procedures**

§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).

*Former Employee and Form Vendors with Enabled Accounts*
*Terminated employees and vendors should have their accounts disabled to prevent potential unauthorized access to ePHI.  The following active accounts designated as former employees or former vendors were identified.  These accounts should be disabled or removed.*

CORP.MYCO.COM

| Username | Name | Status |
|----------|------|--------|
| kmayhem | Kevin Mayhem | Former Employee |
| mSUMMER | Mark SUMMER | Former Employee |
| Pkrickey | Paul Krickey | Former Employee |
| rtaylor | Rob Taylor | Former Vendor |

*Potential Former Employee and Form Vendors with Enabled Accounts*
**The following user accounts were found to not have user activity in the past 30 days and could be an indication of an account that should be disabled.  Security exceptions for these accounts can be found in the Security Exception Worksheet.**

CORP.MYCO.COM

| Username | Name | Current Status | Last Login |
|----------|------|----------------|-----------|
| ASPNET | ASPNET | Employee - no ePHI authorization | <never> |
| bvinings | Bob Vinings | Employee - no ePHI authorization | 2/23/2014 10:46:27 PM |
| bgelding | Beth Gelding | Employee - no ePHI authorization | <never> |
| bminor | Brad Minor | Employee - no ePHI authorization | 11/19/2012 12:34:25 PM |
| DEV$ | DEV$ | Employee - no ePHI authorization | <never> |
| HJoel | Hank Joel | Employee - no ePHI authorization | 9/20/2013 4:55:58 AM |
| IUSR_DC02 | IUSR_DC02 | Employee - no ePHI authorization | 10/12/2009 10:53:59 AM |
| IUSR_STEINBRENNER | IUSR_STEINBRENNER | Employee - no ePHI authorization | 4/11/2012 11:58:18 AM |
| IWAM_DC02 | IWAM_DC02 | Employee - no ePHI authorization | 4/30/2009 4:16:41 PM |
| IWAM_STEINBRENNER | IWAM_STEINBRENNER | Employee - no ePHI authorization | <never> |
| jCradel | Joe Cradel | Employee - no ePHI | 1/22/2014 2:31:34 AM |

| | | authorization | |
|---|---|---|---|
| kglass | K glass | Employee - no ePHI authorization | <never> |
| kmayhem1 | k mayhem1 | Employee - no ePHI authorization | <never> |
| mWEST | Madeleine WEST | Employee - no ePHI authorization | 1/15/2014 3:18:12 AM |
| NetScanner | Net Scanner - MyCo | Employee - no ePHI authorization | 7/20/2012 5:35:23 PM |
| netvendor | NETVENDOR | Employee - no ePHI authorization | <never> |
| hr | MyCo HR | Employee - no ePHI authorization | <never> |
| partners | MyCo Managed Services Partners | Employee - no ePHI authorization | <never> |
| info | MyCo PR | Employee - no ePHI authorization | <never> |
| prsales | MyCo Sales | Employee - no ePHI authorization | <never> |
| support | MyCo Support Team | Employee - no ePHI authorization | 11/5/2011 7:22:27 PM |
| PGK Test1 | PGK Test1 | Employee - no ePHI authorization | 12/16/2012 11:50:51 PM |
| QBDataServiceUser19 | Quickbooks Service Account | Employee - no ePHI authorization | 12/24/2009 12:01:30 PM |
| rtaylor | Rob Taylor | Former Vendor | 1/30/2014 10:29:23 AM |
| smurray | Sarah Murray | Employee - no ePHI authorization | 12/23/2013 1:34:41 PM |
| SUPPORT$ | SUPPORT$ | Employee - no ePHI authorization | <never> |
| marcustest | Test User | Employee - no ePHI authorization | 12/11/2012 9:39:17 AM |

**4.3 - Establish Clear Job Description and Responsibilities / Access Authorization**

§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.

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 and Share Permission Report by User 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 |
| **\\STORAGE01\Common** **(D:\Shared Files\Common)** | **Has ePHI** | Disk | **Everyone** | | ✔ | ✔ |
| | | | BUILTIN\Administrators | ✔ | ✔ | ✔ |

*File System Permissions for Share with ePHI*

| 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 |
| \\STORAGE01\Common (D:\Shared Files\Common) | Disk | CREATOR OWNER | FullControl | Allow |
| | | NT AUTHORITY\SYSTEM | FullControl | Allow |
| | | BUILTIN\Administrators | FullControl | Allow |
| | | MYCO\Domain Admins | FullControl | Allow |
| | | MYCO\Domain Users | FullControl | Allow |
| | | MYCO\sboardroom | FullControl | Allow |
| | | MYCO\RLindy | FullControl | Allow |
| | | MYCO\dHAROLD | FullControl | Allow |
| | | MYCO\kjames | FullControl | Allow |
| | | BUILTIN\Administrators | FullControl | Allow |
| | | MYCO\Domain Admins | FullControl | Allow |
| | | CREATOR OWNER | FullControl | Allow |
| | | NT AUTHORITY\SYSTEM | FullControl | Allow |
| | | BUILTIN\Users | CreateFiles, Synchronize | Allow |

| Share | Share Type | User/Group | File System Permissions | Type |
|---|---|---|---|---|
| | | BUILTIN\Users | AppendData, Synchronize | Allow |
| | | BUILTIN\Users | ReadAndExecute, Synchronize | 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.

The policy and procedure related to authorizing access to ePHI is included with this assessment for reference.

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

**4.5 - Password Management**

§164.308(a)(5)(ii)(d): Security Awareness and Training - 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 | Only 83% consistent ( based on 2 computers sampled) | |
| Enforce password history | 24 passwords remembered | DC01 |
| | 0 passwords remembered | TANDEM |
| Maximum password age | 42 days | All Sampled |
| Minimum password age | 1 days | All Sampled |
| Minimum password length | 7 characters | All Sampled |
| Password must meet complexity requirements | Enabled | 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, ASPNET, BKRICKEY, byellin, bvinings, bgelding, bhanks, cwoods, dHAROLD, dbard, echristy, fthomas, Guest, HJoel, IUSR_DC02, IUSR_STEINBRENNER, IWAM_DC02, IWAM_STEINBRENNER, JDAVIS, JPoole, jpane, jterencel, kglass, kmayhem1, kjacobs, kjames, kmayhem, TWilliams, mparish, mgarrison, mSUMMER, mshoals, mELKINS, mMAYHEMON, mDAVIS, NetScanner, netvendor, pSIMPSON, Pkrickey, support, PGK Test1, QBDataServiceUser19, rjohnson, rphillis, rtaylor, RLindy, sRammond, smurray, SharePointSQL, sLOW, sboardroom, SUPPORT_388945a0, tHenderson, testuser, marcustest, TestV, thughes, wmathers, 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 | MYCO\OPS001 | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.11 | MYCO\MWEST-WIN864 | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.18 | MYCO\PSIMPSON-WIN764 | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.19 | MYCO\SLOW-WIN7 | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.20 | MYCO\SE-DAVIS | Strong Security<br>Administrator - Disabled<br>Guest - Weak, Disabled |
| 10.0.7.26 | MYCO\MELKINS-HP | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.27 | MYCO\HV02 | Strong Security<br>Guest - Weak, Disabled |
| 10.0.7.28 | MYCO\TANDEM | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.29 | MYCO\MARKETING-1 | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.31 | MYCO\MMAYHEMON1 | Strong Security<br>Guest - Weak, Disabled |
| 10.0.7.32 | MYCO\PSIMPSON1 | Potential Risk<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled<br>pablo - Does not meet account policy |
| 10.0.7.43 | MYCO\ISA1 | Strong Security<br>Guest - Weak, Disabled<br>SUPPORT_388945a0 - Disabled |
| 10.0.7.44 | MYCO\JIM-WIN8 | Strong Security<br>Administrator - Disabled<br>Guest - Weak, Disabled |
| 10.0.7.47 | MYCO\REX | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.53 | MYCO\DEV_2012-CORE | Strong Security<br>Guest - Weak, Disabled |
| 10.0.7.54 | MYCO\PKWIN8 | Strong Security<br>Administrator - Weak, Disabled |

| IP Address | Computer Name | Assessment |
|---|---|---|
| | | Guest - Weak, Disabled |
| 10.0.7.57 | MYCO\RANCOR | Strong Security<br>Guest - Disabled |
| 10.0.7.60 | MYCO\PABUILD | Strong Security<br>Guest - Weak, Disabled<br>SUPPORT_388945a0 - Disabled |
| 10.0.7.61 | MYCO\HV05 | Strong Security<br>Guest - Weak, Disabled |
| 10.0.7.62 | MYCO\DEVWIKI | Strong Security<br>Guest - Weak, Disabled<br>SUPPORT_388945a0 - Disabled |
| 10.0.7.63 | MYCO\JIM-WIN7 | Potential Risk<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled<br>jim - Does not meet account policy |
| 10.0.7.65 | MYCO\MYCO30DEV | Potential Risk<br>Guest - Weak, Disabled<br>TsInternetUser - Access denied. |
| 10.0.7.67 | MYCO\JAGA | Strong Security<br>Guest - Weak, Disabled<br>SUPPORT_388945a0 - Disabled |
| 10.0.7.69 | MYCO\DEVTFS | Strong Security<br>Guest - Weak, Disabled |
| 10.0.7.74 | MYCO\BKRICKEY-WIN7 | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.75 | MYCO\DEVWIKI | Strong Security<br>Guest - Weak, Disabled<br>SUPPORT_388945a0 - Disabled |
| 10.0.7.82 | MYCO\PSIMPSON-WIN7TEST | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.90 | MYCO\JOES-PC | Strong Security<br>Administrator - Weak, Disabled<br>Guest - Weak, Disabled |
| 10.0.7.100 | MYCO\PABUILD | Strong Security<br>Guest - Weak, Disabled<br>SUPPORT_388945a0 - Disabled |

**4.6 - 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 | 1 | TANDEM |
| >15 | 0 | |
| Not Enabled | 1 | DC01 |

**4.7 - 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 |

**4.8 - 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 | None |

**The authentication mechanism in place may not be sufficient to prevent a breach.  Immediate attention is required.**

# 5 - Servers and Local Computers

## 5.1 - Protection Against Malicious Software

§164.308(a)(5)(ii)(B): Security Awareness and Training - 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, which is then categorized by domain membership.

Values in the "Name" column contain 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", ✖ indicates "no", and <empty> indicates that a status was not available.

## *CORP.MYCO.COM*

| Computer Name | Antivirus | | | Antispyware | | | Firewall | | Backup | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Name | On | Current | Name | On | Current | Name | On | Name | On |
| 1RB11D1 | | | | | | | | | | |
| AGENT003-PC | | | | | | | | | | |
| APPV-MGMT-SRV | | | | | | | | | | |
| ATLDC01 | | | | | | | | | | |
| BHANKS-LTV | | | | | | | | | | |
| BKRICKEY-WIN7 | ⚙️GFI Languard | ✔ | | ⚙️GFI Languard | ✔ | | 🛡️Windows Firewall | ✔ | None | |
| | 🛡️GFI Software VIPRE | ✔ | ✖ | 🛡️GFI Software VIPRE | ✔ | ✖ | | | | |
| | | | | 🛡️Windows Defender | ✖ | ✔ | | | | |
| BEN | | | | | | | | | | |
| CLOVEPOWER | | | | | | | | | | |
| CLUSTHV01 | | | | | | | | | | |
| CONFERENCE1 | | | | | | | | | | |
| CONFERENCEROOM | | | | | | | | | | |
| CRADEL-SG | | | | | | | | | | |
| D620-5P9W0C1 | | | | | | | | | | |
| D620-8BCJVD1 | | | | | | | | | | |
| DC01 | None | | | None | | | 🛡️Windows Firewall | ✖ | None | |
| DC02 | None | | | None | | | 🛡️Windows Firewall | ✔ | None | |

| Computer Name | Antivirus | | | Antispyware | | | Firewall | | Backup | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Name | On | Current | Name | On | Current | Name | On | Name | On |
| DC03 | None | | | None | | | 🛡Windows Firewall | ✔ | None | |
| DELL_OFFICE | | | | | | | | | | |
| DELL120720 | | | | | | | | | | |
| DEMO5 | | | | | | | | | | |
| DEONNE | | | | | | | | | | |
| DEV_2012-CORE | None | | | None | | | 🛡Windows Firewall | ✔ | None | |
| DEVTFS | None | | | None | | | 🛡Windows Firewall | ✖ | None | |
| DEVWIKI | None | | | None | | | 🛡Windows Firewall | ✖ | ⚙Backup Exec | ✔ |
| DHAROLD-PC | | | | | | | | | | |
| DIALTONE | | | | | | | | | | |
| DAVIS | | | | | | | | | | |
| DAVIS-XP | 🛡Windows Defender | ✔ | ✔ | 🛡Windows Defender | ✔ | ✔ | 🛡Windows Firewall | ✔ | None | |
| DWILLIAMS2 | | | | | | | | | | |
| EHAMMOND-WIN7 | | | | | | | | | | |
| ENGINEERS | | | | | | | | | | |
| ENTCERTS | | | | | | | | | | |
| EPTOWER | | | | | | | | | | |
| ERPI-MYCO-01 | | | | | | | | | | |
| EXCHANGE2013 | | | | | | | | | | |
| FILE2012-1 | None | | | None | | | 🛡Windows Firewall | ✔ | None | |
| FTDELLLAPTOP | | | | | | | | | | |
| FTDESKTOPWORK | | | | | | | | | | |
| FT-LENOVO | | | | | | | | | | |
| GHAMMOND-LT | | | | | | | | | | |
| HJOEL-VM-WIN764 | | | | | | | | | | |
| HJOEL-WIN764 | | | | | | | | | | |
| HP01 | | | | | | | | | | |
| HP02 | | | | | | | | | | |
| HPV00 | | | | | | | | | | |
| 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 | |
| HV2012-1 | | | | | | | | | | |
| HYPERV | | | | | | | | | | |
| HYPERV01 | | | | | | | | | | |
| HYPERV-02 | | | | | | | | | | |

| Computer Name | Antivirus | | | Antispyware | | | Firewall | | Backup | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Name | On | Current | Name | On | Current | Name | On | Name | On |
| HYPERV-03 | | | | | | | | | | |
| ISA1 | | | | | | | | | | |
| JAGA | None | | | None | | | Windows Firewall | ✖ | None | |
| JAMIE-PC | | | | | | | | | | |
| 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 | |
| KMAYHEM1 | | | | | | | | | | |
| LEE | | | | | | | | | | |
| MARKETING-1 | None | | | Windows Defender | ✓ | ✓ | Windows Firewall | ✓ | None | |
| MEGATRON | | | | | | | | | | |
| MELKINS-HP | Windows Defender | ✓ | ✓ | Windows Defender | ✓ | ✓ | Windows Firewall | ✓ | None | |
| MIGTEST | | | | | | | | | | |
| MMAYHEMON | | | | | | | | | | |
| MMAYHEMON1 | None | | | Windows Defender | ✖ | ✓ | None | | None | |
| MMAYHEMON-HP | | | | | | | | | | |
| MWEST-WIN864 | Windows Defender | ✓ | ✓ | Windows Defender | ✓ | ✓ | Windows Firewall | ✓ | None | |
| MSHOALS | | | | | | | | | | |
| MSHELLY1 | | | | | | | | | | |
| MSUMMER | | | | | | | | | | |
| MSUMMERLAPTOP | | | | | | | | | | |
| MSUMMER-LT | | | | | | | | | | |
| NAGATEWAY | | | | | | | | | | |
| NETSCAN01 | | | | | | | | | | |
| OPS001 | Windows Defender | ✓ | ✓ | Windows Defender | ✓ | ✓ | Windows Firewall | ✓ | None | |
| PABUILD | None | | | None | | | Windows Firewall | ✖ | None | |
| PEACH | | | | | | | | | | |
| MYCOROOTAUTH | None | | | None | | | Windows Firewall | ✖ | None | |
| PERFORMA-HLI4PQ | | | | | | | | | | |
| MyCohq | | | | | | | | | | |
| PERSHING-PIT | | | | | | | | | | |
| MYCO-ATL-CORE | None | | | None | | | Windows Firewall | ✖ | None | |
| MYCO-ATL-HPV01 | | | | | | | | | | |
| MYCO-ATL-RJLLTP | | | | | | | | | | |
| MYCO-ATL-WS01 | | | | | | | | | | |
| MYCO-INSPIRON1 | | | | | | | | | | |
| PITMS-LT1 | | | | | | | | | | |

| Computer Name | Antivirus | | | Antispyware | | | Firewall | | Backup | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Name | On | Current | Name | On | Current | Name | On | Name | On |
| MYCO-SCB-LTP | | | | | | | | | | |
| PITWS-PK | | | | | | | | | | |
| pkrickey1 | | | | | | | | | | |
| PKWIN7ENT | | | | | | | | | | |
| PKWin8 | Windows Defender | ✓ | ✓ | Windows Defender | ✓ | ✓ | Windows Firewall | ✓ | None | |
| MYCO30DEV | None | | | None | | | None | | None | |
| MYCODEMO | | | | | | | | | | |
| MYCONMS-BDF | | | | | | | | | | |
| MYCOPATCH | | | | | | | | | | |
| PS01 | | | | | | | | | | |
| PSIMPSON1 | None | | | None | | | Windows Firewall | ✗ | None | |
| PSIMPSON-WIN7 | | | | | | | | | | |
| PSIMPSON-WIN764 | Windows Defender | ✗ | ✓ | Windows Defender | ✗ | ✓ | Windows Firewall | ✓ | None | |
| PSIMPSON-WIN7TEST | None | | | Windows Defender | ✓ | ✓ | Windows Firewall | ✓ | None | |
| QB02 | | | | | | | | | | |
| QBSERVER | | | | | | | | | | |
| RANCOR | Windows Defender | ✓ | ✓ | Windows Defender | ✓ | ✓ | Windows Firewall | ✗ | None | |
| MYCO | | | | | | | | | | |
| REMOTE | | | | | | | | | | |
| REX | Microsoft Security Essentials | ✓ | ✓ | Microsoft Antimalware | ✓ | | Windows Firewall | ✗ | None | |
| | | | | Microsoft Security Essentials | ✓ | ✓ | | | | |
| | | | | Windows Defender | ✗ | ✓ | | | | |
| ROBERT-PC | | | | | | | | | | |
| RS01 | | | | | | | | | | |
| RS02 | | | | | | | | | | |
| SALES01 | | | | | | | | | | |
| SBLAPTOP | | | | | | | | | | |
| SE-DAVIS | None | | | Windows Defender | ✗ | ✓ | Windows Firewall | ✓ | ShadowProtect | ✓ |
| | | | | | | | | | StorageCraft | ✗ |
| SHAREPOINT-01 | None | | | None | | | Windows Firewall | ✓ | None | |
| SHAREPOINT1 | | | | | | | | | | |
| SHARLISE-WIN8 | | | | | | | | | | |
| SHELDON | | | | | | | | | | |
| SHREDDER | | | | | | | | | | |
| SLOW-WIN8 | GFI Languard | ✓ | | GFI Languard | ✓ | | Windows Firewall | ✓ | None | |

| Computer Name | Antivirus | | | Antispyware | | | Firewall | | Backup | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Name | On | Current | Name | On | Current | Name | On | Name | On |
| | 🛡GFI Software VIPRE | ✔ | ✖ | 🛡GFI Software VIPRE | ✔ | ✖ | | | | |
| | 🛡Windows Defender | ✖ | ✔ | 🛡Windows Defender | ✖ | ✔ | | | | |
| SQL2012-01 | None | | | None | | | 🛡Windows Firewall | ✔ | None | |
| STARSCREAM | | | | | | | | | | |
| STARTEAM | | | | | | | | | | |
| STORAGE01 | None | | | None | | | 🛡Windows Firewall | ✖ | None | |
| TANDEM | None | | | 🛡Windows Defender | ✔ | ✖ | 🛡Windows Firewall | ✔ | None | |
| TESTSERVER1 | | | | | | | | | | |
| TESTXP01 | | | | | | | | | | |
| THRASH2 | | | | | | | | | | |
| USAL9K49RH1 | | | | | | | | | | |
| USER-PC23 | | | | | | | | | | |
| UTIL01 | None | | | None | | | 🛡Windows Firewall | ✖ | None | |
| UTIL12 | None | | | None | | | 🛡Windows Firewall | ✔ | None | |
| VM1-WIN2003 | | | | | | | | | | |
| VM2-2003 | | | | | | | | | | |
| VM-JDAVIS-WIN7 | | | | | | | | | | |
| VM-WIN2003 | | | | | | | | | | |
| VM-WIN7 | | | | | | | | | | |
| VM-WIN7-2 | | | | | | | | | | |
| VM-WIN7-3 | | | | | | | | | | |
| VM-WIN8BETA | | | | | | | | | | |
| W2012TEST | | | | | | | | | | |
| WIN2008 | | | | | | | | | | |
| WIN2008R2 | | | | | | | | | | |
| WIN7ULT | | | | | | | | | | |
| WINDESKTOP | | | | | | | | | | |
| WIN-HNQ8G0O1RAI | | | | | | | | | | |
| WINXP32 | | | | | | | | | | |
| WINXP64 | | | | | | | | | | |
| wmathers1 | | | | | | | | | | |

## No Domain

| Computer Name | Antivirus | | | Antispyware | | | Firewall | | Backup | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Name | On | Current | Name | On | Current | Name | On | Name | On |
| sLOW-win7.corp.MyCo.com | None | | | 🛡Windows Defender | ✔ | ✔ | 🛡Windows Firewall | ✔ | None | |

**Endpoint Security Assessment**

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

**<u>30 computers</u> were detected as having no anti-virus or anti-spyware.**

**<u>4 computers</u> with active but out of date anti-virus or anti-spyware.**

*Security Patch Summary*

This section contains the patching status of computers using MBSA to determine need. Computers with missing patches are highlighted in red.

IP Range for MBSA scan: 10.0.7.0-10.0.7.255

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

| IP Address | Computer Name | Issue | Score | Assessment |
|---|---|---|---|---|
| 10.0.7.26 | MYCO\MELKINS-HP | Security Updates | Unable to scan | Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. |
| **10.0.7.27** | **MYCO\HV02** | SQL Server Security Updates | Check passed | No security updates are missing. |
| | | **Windows Security Updates** | **Check failed (critical)** | **9 security updates are missing. 2 service packs or update rollups are missing.** |
| 10.0.7.28 | MYCO\TANDEM | Security Updates | Unable to scan | Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. |
| 10.0.7.29 | MYCO\MARKETING-1 | Security Updates | Unable to scan | Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. |
| **10.0.7.31** | **MYCO\MMAYHEMON1** | Bing Security Updates | Check passed | No security updates are missing. |
| | | **Developer Tools, Runtimes, and Redistributables Security Updates** | **Check failed (critical)** | **1 security updates are missing.** |
| | | **Microsoft Lync Server and Microsoft Lync Security Updates** | **Check failed (critical)** | **1 security updates are missing. 1 service packs or update rollups are missing.** |
| | | **Office Security Updates** | **Check failed (critical)** | **15 security updates are missing.** |
| | | Office Communications Server And Office Communicator Security Updates | Check passed | No security updates are missing. |
| | | SQL Server Security Updates | Check passed | No security updates are missing. |
| | | **Silverlight Security Updates** | **Check failed (critical)** | **1 security updates are missing.** |
| | | **Windows Security Updates** | **Check failed (critical)** | **67 security updates are missing. 2 service packs or update rollups are missing.** |
| 10.0.7.32 | MYCO\PSIMPSON1 | Developer Tools, Runtimes, and Redistributables Security Updates | Check passed | No security updates are missing. |
| | | Office Security Updates | Check passed | No security updates are missing. |
| | | SDK Components Security Updates | Check passed | No security updates are missing. |
| | | SQL Server Security Updates | Check passed | No security updates are missing. |
| | | Silverlight Security Updates | Check passed | No security updates are missing. |
| | | Windows Security Updates | Check passed | No security updates are missing. |
| **10.0.7.43** | **MYCO\ISA1** | **Internet Security and Acceleration Server Security Updates** | **Check failed (critical)** | **1 security updates are missing. 1 service packs or update rollups are missing.** |
| | | **SQL Server Security Updates** | **Check failed (critical)** | **1 security updates are** |

| IP Address | Computer Name | Issue | Score | Assessment |
|---|---|---|---|---|
| | | | | **missing.** |
| | | **Windows Security Updates** | **Check failed (critical)** | **15 security updates are missing. 2 service packs or update rollups are missing.** |
| 10.0.7.44 | MYCO\JIM-WIN8 | Security Updates | Unable to scan | Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. |
| **10.0.7.47** | **MYCO\REX** | **Developer Tools, Runtimes, and Redistributables Security Updates** | **Check failed (critical)** | **3 security updates are missing.** |
| | | **Microsoft Lync Server and Microsoft Lync Security Updates** | **Check failed (critical)** | **1 security updates are missing. 1 service packs or update rollups are missing.** |
| | | **Office Security Updates** | **Check failed (critical)** | **32 security updates are missing. 2 service packs or update rollups are missing.** |
| | | Office Communications Server And Office Communicator Security Updates | Check passed | No security updates are missing. |
| | | SDK Components Security Updates | Check passed | No security updates are missing. |
| | | SQL Server Security Updates | Check failed (non-critical) | 1 service packs or update rollups are missing. |
| | | **Silverlight Security Updates** | **Check failed (critical)** | **1 security updates are missing.** |
| | | **Windows Security Updates** | **Check failed (critical)** | **69 security updates are missing. 4 service packs or update rollups are missing.** |
| 10.0.7.57 | MYCO\RANCOR | Developer Tools, Runtimes, and Redistributables Security Updates | Check passed | No security updates are missing. |
| | | Office Security Updates | Check passed | No security updates are missing. |
| | | SDK Components Security Updates | Check passed | No security updates are missing. |
| | | SQL Server Security Updates | Check passed | No security updates are missing. |
| | | Silverlight Security Updates | Check passed | No security updates are missing. |
| | | Windows Security Updates | Check passed | No security updates are missing. |
| 10.0.7.60 | MYCO\PABUILD | Security Updates | Unable to scan | Computer has an older version of the client and security database demands a newer version. Current version is and minmum required version is . |
| **10.0.7.62** | **MYCO\DEVWIKI** | **Windows Security Updates** | **Check failed (critical)** | **130 security updates are missing. 5 service packs or update rollups are missing.** |
| 10.0.7.63 | MYCO\JIM-WIN7 | Security Updates | Unable to scan | Cannot contact Windows Update Agent on target computer, possibly due to |

| IP Address | Computer Name | Issue | Score | Assessment |
|---|---|---|---|---|
| | | | | firewall settings. |
| 10.0.7.65 | MYCO\MYCO30DEV | Security Updates | Unable to scan | Cannot load security CAB file. |
| 10.0.7.67 | MYCO\JAGA | Security Updates | Unable to scan | Cannot load security CAB file. |
| 10.0.7.74 | MYCO\BKRICKEY-WIN7 | Security Updates | Unable to scan | Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. |
| **10.0.7.75** | **MYCO\DEVWIKI** | **Windows Security Updates** | **Check failed (critical)** | **130 security updates are missing. 5 service packs or update rollups are missing.** |
| 10.0.7.82 | MYCO\PSIMPSON-WIN7TEST | Security Updates | Unable to scan | Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. |
| 10.0.7.90 | MYCO\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 <u>15 computers</u>.  The computers should be investigated to assure the latest patches have been applied.**

**Security patches are missing on <u>6 computers</u>.  These patches should be applied as soon as possible to prevent or restrict the spread of malicious software.**

**5.2 - Applications and Data Criticality Analysis**

§164.308(a)(7)(ii)-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.

*Copiers and Multi-function Printers*

Our company uses copiers and multi-function printers.

*Cloud-based EHR System*

Our company uses a cloud-based EHR system.

**5.3 - Business Associate Agreements for Cloud Servers and Data Centers**

§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.

**Data Center**

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

Contact Information:              *None provided.*

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

**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 | REX | | Yes | |
| LogMeIn | TANDEM | | Yes | |
| LogMeIn | MWEST-WIN864 | | Yes | |
| LogMeIn | PSIMPSON-WIN764 | | Yes | |
| LogMeIn | PSIMPSON1 | | Yes | |
| TeamViewer | TANDEM | | Yes | |
| TeamViewer | sLOW-win7.corp.MyCo.com | | Yes | |
| TeamViewer | PSIMPSON-WIN764 | | Yes | |
| TeamViewer | MARKETING-1 | | Yes | |
| TeamViewer | RANCOR | | Yes | |
| TeamViewer | SE-DAVIS | | Yes | |
| TeamViewer | PSIMPSON1 | | Yes | |
| ScreenConnect | JAGA | | Yes | |
| ScreenConnect | STORAGE01 | | Yes | |
| ScreenConnect | REX | | Yes | |
| ScreenConnect | BKRICKEY-WIN7 | | Yes | |
| ScreenConnect | HV05 | | Yes | |
| ScreenConnect | HV02 | | Yes | |
| ScreenConnect | HV01 | | Yes | |
| ScreenConnect | HV04 | | Yes | |
| ScreenConnect | HV03 | | Yes | |
| ScreenConnect | DC01 | | Yes | |
| ScreenConnect | UTIL01 | | Yes | |

# 6 - Firewall

## 6.1 - Access Authorization

§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.

**We employ an external firewall to prevent external attacks.**

Models:

**The external firewall does have an Intrusion Prevention System; however, it is not turned on.**

## 6.2 - Protection Against Malicious Software

§164.308(a)(5)(ii)(B): Security Awareness and Training - 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): Security Awareness and Training - 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 |
|---|---|---|---|---|---|---|---|
| **5.23.4.133 (50-243-217-133-static.hfc.comcastbusiness.net)** | Medium risk | 5 | 0 | **2** | 2 | 0 | 6.9 |
| Total: 1 | Medium risk | 5 | 0 | **2** | 2 | 0 | 6.9 |

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.

# 7 - Email

## 7.1 - Applications and Data Criticality Analysis

§164.308(a)(7)(ii)-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 | Outlook Data File - wparson@Excelsior.com.ost<br>wparson@MyCo.com - wparson@MyCo.com.ost<br>imap.googlemail.com.msf<br>Archives.msf<br>Drafts.msf<br>Follow up.msf<br>INBOX.msf<br>Misc.msf<br>Priority.msf<br>Sent.msf<br>Templates.msf<br>[Gmail].msf<br>All Mail.msf | |

## 8 - Wireless

### 8.1 - Access Authorization

§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.

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 |
|---|---|---|---|
| *No wireless networks detected* | | | |

***Guest Wireless***

We do offer guest wireless to visitors or patients.

**<span style="color:red">Guest wireless is on the same network as ePHI.</span>**

### 8.2 - Access Establishment

§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 wireless keys were last changed **25 days ago**.

### 8.3 - Workforce Security

§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).

The wireless key has been changed since the latest high risk employee termination.