HIPAA Assessment

Evidence of HIPAA Policy Compliance

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

Prepared for: Client Company

Prepared by: AMS Networks

Table of Contents

06 Firewall

07 Email

08 Wireless

09 Business Associates

10 Administrative, Physical, and Technical Safeguard Policies and Procedures

11 Privacy Rule

12 Breach Notification Rule

1 - Overview

Our organization has adopted written Policies & Procedures referenced in Section 10 - Administrative, Physical, and Technical Safeguard Policies and 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:

Tel: 555-555-1000
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 documents.

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: Unattended laptop computers are not secured.

Data Storage Devices

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

Comments: CD-ROMs labeled as data backups were lying out in the open.

Public Viewable Screens

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

Comments: Workforce member computers have displays facing the offices East window.

Retired/Decommissioned/Failed Systems or Storage Devices

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

Comments: 14 computer workstations were identified as being retired. The data on the computer disks was encrypted prior to the computer disks being destroyed for each workstation.

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	86	0
Employee - no ePHI authorization	0	0
Vendor - ePHI authorization	0	0
Vendor - no ePHI authorization	0	0
Former Employee	0	0
Former Vendor	0	0
Service Account	0	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

GENERIC ACCOUNT	FIRST NAME	LAST NAME	COMPUTER	IP ADDRESS
Administrator				

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).

Former Employees and 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.

USERNAME	NAME	ACCESS	STATUS
No accounts			

Potential Former Employees and Vendors with Enabled Accounts

The following user accounts were found to not have user activity in the past 90 days. This could be an indication that the accounts should be disabled.

Security exceptions for these accounts can be found in the Security Exception Worksheet

myclientsnetwork.com

USERNAME	NAME	CURRENT STATUS	LAST LOGIN
Ajwfrcmbr	A Jensen	Employee - ePHI authorization	
Arom	Axel Rom	Employee - ePHI authorization	
Administrator	Administrator	Employee - ePHI authorization	7/8/2020 2:01:00 PM
dwwfrcmbr	D White	Employee - ePHI authorization	
Ebaldwin	Edward Baldwin	Employee - ePHI authorization	3/12/2019 10:12:29 AM
fowardslash	fowared slash	Employee - ePHI authorization	
jknightling	Jorge Knightling	Employee - ePHI authorization	3/12/2019 10:14:12 AM
jasus	Jeremy Asus	Employee - ePHI	3/12/2019 10:13:48

USERNAME	NAME	CURRENT STATUS	LAST LOGIN
		authorization	AM
jgilligan	Janet Gross	Employee - ePHI authorization	
jkalo	Jorge Knightling	Employee - ePHI authorization	3/12/2019 11:05:47 AM
jchestnut	Janet Chestnut	Employee - ePHI authorization	3/12/2019 10:53:17 AM
jconway	Joseph Conway	Employee - ePHI authorization	1/22/2019 9:37:23 AM
jdelaney	Jonah Delaney	Employee - ePHI authorization	3/12/2019 10:46:12 AM
mwwfrcmbr	M Warly	Employee - ePHI authorization	
mjohnson	Maxwell Johnson	Employee - ePHI authorization	3/12/2019 10:45:56 AM
mtalman	M Talman	Employee - ePHI authorization	2/8/2019 11:01:16 AM
pwalker	Paula Walker	Employee - ePHI authorization	3/12/2019 10:13:25 AM
pswfrcmbr	P Sulu	Employee - ePHI authorization	6/27/2019 8:34:54 AM
sjane	Sonny Jane	Employee - ePHI authorization	3/12/2019 10:45:44 AM
tshelman	Terri Shelman	Employee - ePHI authorization	3/12/2019 10:12:52 AM
uwfrcmbr	unitbdr admin	Employee - ePHI authorization	

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
\\DCTLR01\NETLOGON (C:\Windows\SYSVOL\sysvol\myclientsnetwork.com\SCRIPTS)	**Has ePHI**	Disk	**Everyone**	×	×	✓
			BUILTIN\Administrators	✓	✓	✓
\\DCTLR01\SYSVOL (C:\Windows\SYSVOL\sysvol)	**Has ePHI**	Disk	**Everyone**	×	×	✓
			BUILTIN\Administrators	✓	✓	✓
			NT AUTHORITY\Authenticated Users	✓	✓	✓
\\DCTLR02\NETLOGON (C:\Windows\SYSVOL\sysvol\myclientsnetwork.com\SCRIPTS)	**Has ePHI**	Disk	**Everyone**	×	×	✓
			BUILTIN\Administrators	✓	✓	✓
\\DCTLR02\SYSVOL (C:\Windows\SYSVOL\sysvol)	**Has ePHI**	Disk	**Everyone**	×	×	✓
			BUILTIN\Administrators	✓	✓	✓
			NT AUTHORITY\Authenticated Users	✓	✓	✓
\\DESKPC-RB3LBP3\print$ (C:\Windows\system32\spool\drivers)	**Has ePHI**	Disk	**Everyone**	×	×	✓
			BUILTIN\Administrators	✓	✓	✓
\\FILESVR01\Accounting (D:\Shares\Accounting)	**Has ePHI**	Disk	**Everyone**	✓	✓	✓
\\FILESVR01\Human Resources (D:\Shares\Human Resources)	**Has ePHI**	Disk	**Everyone**	✓	✓	✓

SHARE	EPHI	SHARE TYPE	USER/GROUP	SHARE PERMISSIONS		
				FULL CONTROL	CHANGE	READ
\\FILESVR01\Operations (D:\Shares\Operations)	**Has ePHI**	Disk	BUILTIN\Administrators **Everyone**	✓ ✓	✓ ✓	✓ ✓
\\FILESVR01\Test Data (D:\Shares\Test Data)	**Has ePHI**	Disk	**Everyone**	✓	✓	✓
\\FILESVR01\Work Folders (D:\Shares\Work Folders)	**Has ePHI**	Disk	**Everyone**	✓	✓	✓
\\HVSVR1\Operations (H:\Shares\Operations)	**Has ePHI**	Disk	**Everyone**	✓	✓	✓
\\HVSVR2\Operations (H:\Shares\Operations)	**Has ePHI**	Disk	**Everyone**	✓	✓	✓
\\SQLSVR02\DEVTESTSQL (\\?\GLOBALROOT\Device\RsFx0401\<localmachine>\DEVTESTSQL)	**Has ePHI**	Disk	NT AUTHORITY\Authenticated Users	✓	✓	✓

File System Permissions for Share with ePHI

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
\\APPSVR01\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\APPSVR01\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
\\APPSVR01\IPC$	IPC, Special			
\\DCTLR01\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES		
\\DCTLR01\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
\\DCTLR01\IPC$	IPC, Special			
\\DCTLR01\NETLOGON (C:\Windows\SYSVOL\sysvol\myclientsnetwork.com\SCRIPTS)	Disk	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\Authenticated Users	Special (-1610612736)	Allow
		NT AUTHORITY\Authenticated Users	ReadAndExecute, Synchronize	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	Special (268435456)	Allow
		BUILTIN\Administrators	Write, ReadAndExecute, ChangePermissions, TakeOwnership, Synchronize	Allow
		BUILTIN\Server Operators	Special (-1610612736)	Allow
		BUILTIN\Server Operators	ReadAndExecute, Synchronize	Allow
\\DCTLR01\SYSVOL (C:\Windows\SYSVOL\sysvol)	Disk	CREATOR OWNER	Special (-536084480)	Allow
		NT AUTHORITY\Authenticated Users	Special (-1610612736)	Allow
		NT AUTHORITY\Authenticated Users	ReadAndExecute, Synchronize	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	Special (-536084480)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		BUILTIN\Administrators	Write, ReadAndExecute, ChangePermissions, TakeOwnership, Synchronize	Allow
		BUILTIN\Server Operators	Special (-1610612736)	Allow
		BUILTIN\Server Operators	ReadAndExecute, Synchronize	Allow
\\DCTLR02\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DCTLR02\C$ (C:\)	Special	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	AppendData	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		BUILTIN\Users	CreateFiles	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\DCTLR02\IPC$	IPC, Special			
\\DCTLR02\NETLOGON (C:\Windows\SYSVOL\sysvol\myclientsnetwork.com\SCRIPTS)	Disk	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\Authenticated Users	Special (-1610612736)	Allow
		NT AUTHORITY\Authenticated Users	ReadAndExecute, Synchronize	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	Special (268435456)	Allow
		BUILTIN\Administrators	Write, ReadAndExecute, ChangePermissions, TakeOwnership, Synchronize	Allow
		BUILTIN\Server Operators	Special (-1610612736)	Allow
		BUILTIN\Server Operators	ReadAndExecute, Synchronize	Allow
\\DCTLR02\SYSVOL (C:\Windows\SYSVOL\sysvol)	Disk	CREATOR OWNER	Special (-536084480)	Allow
		NT AUTHORITY\Authenticated Users	Special (-1610612736)	Allow
		NT AUTHORITY\Authenticated Users	ReadAndExecute, Synchronize	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	Special (-536084480)	Allow
		BUILTIN\Administrators	Write, ReadAndExecute, ChangePermissions, TakeOwnership, Synchronize	Allow
		BUILTIN\Server Operators	Special (-1610612736)	Allow
		BUILTIN\Server Operators	ReadAndExecute, Synchronize	Allow
\\DESKPC-09UPSPO\ADMIN$	Special	CREATOR OWNER	Special (268435456)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
(C:\WINDOWS)		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	Modify, Synchronize	Allow
		BUILTIN\Administrators	Special (268435456)	Allow
		BUILTIN\Administrators	Modify, Synchronize	Allow
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-09UPSPO\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
\\DESKPC-09UPSPO\IPC$	IPC, Special			
\\DESKPC-108DSLI\ADMIN$ (C:\Windows)	Special	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		NT AUTHORITY\SYSTEM	Modify, Synchronize	Allow
		BUILTIN\Administrators	Special (268435456)	Allow
		BUILTIN\Administrators	Modify, Synchronize	Allow
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-108DSLI\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
\\DESKPC-108DSLI\IPC$	IPC, Special			
\\DESKPC-191IJQL\ADMIN$ (C:\WINDOWS)	Special	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	Modify, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		BUILTIN\Administrators	Special (268435456)	Allow
		BUILTIN\Administrators	Modify, Synchronize	Allow
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-191IJQL\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
\\DESKPC-191IJQL\IPC$	IPC, Special			
\\DESKPC-1QSHT11\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

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		BUILTIN\Administrators	Modify, Synchronize	Allow
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-1QSHT11\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
\\DESKPC-1QSHT11\IPC$	IPC, Special			
\\DESKPC-3IC4R57\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
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-3IC4R57\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
\\DESKPC-3IC4R57\IPC$	IPC, Special			
\\DESKPC-4171AR0\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
		BUILTIN\Users	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-4171AR0\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
\\DESKPC-4171AR0\IPC$	IPC, Special			
\\DESKPC-4PF2ICP\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute,	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
			Synchronize	
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-4PF2ICP\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
\\DESKPC-4PF2ICP\IPC$	IPC, Special			
\\DESKPC-534MS45\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-534MS45\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
\\DESKPC-534MS45\IPC$	IPC, Special			
\\DESKPC-5GTVFB3\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT	Special (268435456)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		SERVICE\TrustedInstaller		
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-5GTVFB3\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
\\DESKPC-5GTVFB3\IPC$	IPC, Special			
\\DESKPC-7T6GCBK\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-7T6GCBK\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
\\DESKPC-7T6GCBK\IPC$	IPC, Special			
\\DESKPC-85BJGJT\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT	FullControl	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		SERVICE\TrustedInstaller		
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-85BJGJT\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
\\DESKPC-85BJGJT\IPC$	IPC, Special			
\\DESKPC-ADU1DSQ\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-ADU1DSQ\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
\\DESKPC-ADU1DSQ\IPC$	IPC, Special			
\\DESKPC-AMB2RC8\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE	ReadAndExecute,	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		AUTHORITY\ALL APPLICATION PACKAGES	Synchronize	
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-AMB2RC8\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
\\DESKPC-AMB2RC8\IPC$	IPC, Special			
\\DESKPC-B9ETSS8\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-B9ETSS8\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
\\DESKPC-B9ETSS8\IPC$	IPC, Special			
\\DESKPC-BDJFFLG\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-BDJFFLG\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
\\DESKPC-BDJFFLG\IPC$	IPC, Special			
\\DESKPC-E0CVM8B\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-E0CVM8B\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
\\DESKPC-E0CVM8B\IPC$	IPC, Special			
\\DESKPC-ELBLDBS\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		AUTHORITY\ALL APPLICATION PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-ELBLDBS\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
\\DESKPC-ELBLDBS\IPC$	IPC, Special			
\\DESKPC-F0M1O27\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-F0M1O27\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
\\DESKPC-F0M1O27\IPC$	IPC, Special			
\\DESKPC-F6CKERQ\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-F6CKERQ\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
\\DESKPC-F6CKERQ\IPC$	IPC, Special			
\\DESKPC-FEQIJCC\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-FEQIJCC\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
\\DESKPC-FEQIJCC\IPC$	IPC, Special			
\\DESKPC-FOP1ENA\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE	ReadAndExecute,	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Synchronize	
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-FOP1ENA\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
\\DESKPC-FOP1ENA\IPC$	IPC, Special			
\\DESKPC-G0QQU53\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		RESTRICTED APPLICATION PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-G0QQU53\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
\\DESKPC-G0QQU53\IPC$	IPC, Special			
\\DESKPC-H1NN5VD\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-H1NN5VD\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
\\DESKPC-H1NN5VD\IPC$	IPC, Special			
\\DESKPC-HN95P9Q\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-HN95P9Q\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
\\DESKPC-HN95P9Q\IPC$	IPC, Special			
\\DESKPC-HQJ7BG2\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-HQJ7BG2\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
\\DESKPC-HQJ7BG2\IPC$	IPC, Special			
\\DESKPC-I595F9F\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES		
\\DESKPC-I595F9F\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
\\DESKPC-I595F9F\IPC$	IPC, Special			
\\DESKPC-IMMJR2V\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		RESTRICTED APPLICATION PACKAGES		
\\DESKPC-IMMJR2V\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
\\DESKPC-IMMJR2V\IPC$	IPC, Special			
\\DESKPC-LIFRCFU\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGES		
\\DESKPC-LIFRCFU\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
\\DESKPC-LIFRCFU\IPC$	IPC, Special			
\\DESKPC-MA551PF\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		PACKAGES		
\\DESKPC-MA551PF\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
\\DESKPC-MA551PF\IPC$	IPC, Special			
\\DESKPC-MVGNQ06\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
\\DESKPC-MVGNQ06\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
\\DESKPC-MVGNQ06\IPC$	IPC, Special			
\\DESKPC-N883DVI\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-N883DVI\C$	Special	NT	AppendData	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
(C:\)		AUTHORITY\Authenticated Users		
		NT AUTHORITY\Authenticated Users	Special (-536805376)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\DESKPC-N883DVI\IPC$	IPC, Special			
\\DESKPC-NF6BLBC\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-NF6BLBC\C$ (C:\)	Special	NT AUTHORITY\Authenticated	AppendData	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		Users		
		NT AUTHORITY\Authenticated Users	Special (-536805376)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\DESKPC-NF6BLBC\IPC$	IPC, Special			
\\DESKPC-P1C4FJP\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-P1C4FJP\C$ (C:\)	Special	NT AUTHORITY\Authenticated Users	AppendData	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		NT AUTHORITY\Authenticated Users	Special (-536805376)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\DESKPC-P1C4FJP\IPC$	IPC, Special			
\\DESKPC-QFC42PE\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-QFC42PE\C$ (C:\)	Special	NT AUTHORITY\Authenticated Users	AppendData	Allow
		NT	Special (-536805376)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		AUTHORITY\Authenticated Users		
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\DESKPC-QFC42PE\IPC$	IPC, Special			
\\DESKPC-RB3LBP3\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-RB3LBP3\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
\\DESKPC-RB3LBP3\IPC$	IPC, Special			

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
\\DESKPC-RB3LBP3\print$ (C:\Windows\system32\spool\drivers)	Disk	Everyone	ReadAndExecute, Synchronize	Allow
		Everyone	Special (-1610612736)	Allow
		CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	Special (268435456)	Allow
		BUILTIN\Administrators	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
\\DESKPC-U1K3NAF\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\DESKPC-U1K3NAF\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
\\DESKPC-U1K3NAF\IPC$	IPC, Special			
\\EXCHSVR01\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
\\EXCHSVR01\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
\\EXCHSVR01\IPC$	IPC, Special			
\\FILESVR01\Accounting (D:\Shares\Accounting)	Disk	BUILTIN\Administrators	FullControl	Allow
		TEST\Accounting	Modify, Synchronize	Allow
		BUILTIN\Administrators	FullControl	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		CREATOR OWNER	Special (268435456)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		BUILTIN\Users	AppendData	Allow
		BUILTIN\Users	CreateFiles	Allow
\\FILESVR01\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow

		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\FILESVR01\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
\\FILESVR01\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
\\FILESVR01\Human Resources (D:\Shares\Human Resources)	Disk	BUILTIN\Administrators	FullControl	Allow
		TEST\Human Resources	Modify, Synchronize	Allow
		BUILTIN\Administrators	FullControl	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		CREATOR OWNER	Special (268435456)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		BUILTIN\Users	AppendData	Allow
		BUILTIN\Users	CreateFiles	Allow
\\FILESVR01\IPC$	IPC, Special			
\\FILESVR01\Operations (D:\Shares\Operations)	Disk	NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		TEST\dwfrcmbr	FullControl	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
\\FILESVR01\Test Data (D:\Shares\Test Data)	Disk	BUILTIN\Administrators	FullControl	Allow
		TEST\QA	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		CREATOR OWNER	Special (268435456)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		BUILTIN\Users	AppendData	Allow
		BUILTIN\Users	CreateFiles	Allow
\\FILESVR01\Work Folders (D:\Shares\Work Folders)	Disk	NT AUTHORITY\LOCAL SERVICE	FullControl	Deny
		NT AUTHORITY\LOCAL SERVICE	Special (268435456)	Deny
		CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		NT AUTHORITY\SYSTEM	Special (268435456)	Allow
		BUILTIN\Administrators	FullControl	Allow
		TEST\Domain Users	ReadData, AppendData, ExecuteFile, ReadAttributes, WriteAttributes, Synchronize	Allow
		TEST\Domain Users	Modify, Synchronize	Allow
		BUILTIN\Administrators	FullControl	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		CREATOR OWNER	Special (268435456)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		BUILTIN\Users	AppendData	Allow
		BUILTIN\Users	CreateFiles	Allow
\\HVSVR1\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
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\HVSVR1\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
\\HVSVR1\H$ (H:\)	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

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
\\HVSVR1\IPC$	IPC, Special			
\\HVSVR1\Operations (H:\Shares\Operations)	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
\\HVSVR2\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\HVSVR2\C$ (C:\)	Special	CREATOR OWNER	Special (268435456)	Allow
		NT AUTHORITY\SYSTEM	FullControl	Allow
		BUILTIN\Administrators	FullControl	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		BUILTIN\Users	AppendData	Allow
		BUILTIN\Users	CreateFiles	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
\\HVSVR2\H$ (H:\)	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
\\HVSVR2\IPC$	IPC, Special			
\\HVSVR2\Operations (H:\Shares\Operations)	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
\\SQLSVR01\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION	ReadAndExecute, Synchronize	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		PACKAGES		
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
\\SQLSVR01\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
\\SQLSVR01\IPC$	IPC, Special			
\\SQLSVR02\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		RESTRICTED APPLICATION PACKAGES		
\\SQLSVR02\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
\\SQLSVR02\DEVTESTSQL (\\?\GLOBALROOT\Device\RsFx0401\<localmachine>\DEVTESTSQL)	Disk			
\\SQLSVR02\IPC$	IPC, Special			
\\SQLSVR02\S$ (S:\)	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
\\SQLSVR03\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
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\SQLSVR03\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
\\SQLSVR03\IPC$	IPC, Special			
\\SQLSVR03\S$ (S:\)	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
\\WRKSTN10-1\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

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		BUILTIN\Administrators	Modify, Synchronize	Allow
		BUILTIN\Users	Special (-1610612736)	Allow
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\WRKSTN10-1\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
\\WRKSTN10-1\IPC$	IPC, Special			
\\WRKSTN10-2\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
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\WRKSTN10-2\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
\\WRKSTN10-2\IPC$	IPC, Special			
\\WRKSTN10-4\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
		BUILTIN\Users	Special (-1610612736)	Allow

SHARE	SHARE TYPE	USER/GROUP	FILE SYSTEM PERMISSIONS	TYPE
		BUILTIN\Users	ReadAndExecute, Synchronize	Allow
		NT SERVICE\TrustedInstaller	Special (268435456)	Allow
		NT SERVICE\TrustedInstaller	FullControl	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	Special (-1610612736)	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	ReadAndExecute, Synchronize	Allow
		APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	Special (-1610612736)	Allow
\\WRKSTN10-4\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
\\WRKSTN10-4\IPC$	IPC, Special			

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.

§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 receive training on how to avoid becoming a victim of technology threat.

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 another user and should be clearly identified. The following is a list of all users with administrative roles regarding the network environment.

Domain: myclientsnetwork.com

More than 30 % of the users are in the Domain Administrator group and have unfettered access to files and system resources.

USERNAME	NAME	MEMBER OF
abwfrcmbr	A Branaugh	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users
ajwfrcmbr	A Jensen	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users
aswfrcmbr	A Smith	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users
Administrator	Administrator	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users **Enterprise Admins** Group Policy Creator Owners **Schema Admins** Users
dwfrcmbr	Dora Baxter	**admin** **Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users **Enterprise Admins** Group Policy Creator Owners **Schema Admins** Users
dkwfrcmbr	D Kindle	**Administrators**

USERNAME	NAME	MEMBER OF
		Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users
dwwfrcmbr	D White	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users
ecwfrcmbr	Edward C	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users
jswfrcmbr	J Shearing	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users
jwwfrcmbr	J Westerfield	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users
lwwfrcmbr	L Wilson	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users
mgwfrcmbr	M Green	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users
mpwfrcmbr	M Peters	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users
mwwfrcmbr	M Warly	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users
pkwfrcmbr	P Kettering	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users

USERNAME	NAME	MEMBER OF
pswfrcmbr	P Sulu	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users
skwfrcmbr	S Kulynee	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users
spwfrcmbr	S Peters	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users
thwfrcmbr	T Harris	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users
uwfrcmbr	unitbdr admin	**admin** **Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users **Enterprise Admins** Group Policy Creator Owners **Schema Admins** Users
wpwfrcmbr	W Paulson	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users Users
ydwfrcmbr	Yami Dareloth	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users
ylwfrcmbr	Y Leland	**Administrators** Denied RODC Password Replication Group **Domain Admins** Domain Users QA Users

4.6 - Password Management

§164.308(a)(5)(ii)(d): 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.

Password Policy Consistency:	Consistent

POLICY	SETTING	COMPUTERS
Enforce password history	24 passwords remembered	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4
Maximum password age	42 days	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4
Minimum password age	1 days	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4
Minimum password length	7 characters	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4
Minimum password length audit	Not Defined	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4
Password must meet complexity requirements	Enabled	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4
Relax minimum password length limits	Not Defined	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-

		FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06
Store passwords using reversible encryption	Disabled	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4

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

Account Lockout Policy Consistency — Consistent

POLICY	SETTING	COMPUTERS
Account lockout duration	Not Applicable	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4
Account lockout threshold	0 invalid logon attempts	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4
Reset account lockout counter after	Not Applicable	DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4PF2ICP, DESKPC-7T6GCBK, DESKPC-B9ETSS8, DESKPC-FEQIJCC, DESKPC-H1NN5VD, DESKPC-MVGNQ06, WRKSTN10-4

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:

myclientsnetwork.com

ajwfrcmbr, aswfrcmbr, dwfrcmbr, dkwfrcmbr, dwwfrcmbr, ecwfrcmbr, jswfrcmbr, jwwfrcmbr, lwwfrcmbr, mgwfrcmbr, mpwfrcmbr, mwwfrcmbr, mtalman, pkwfrcmbr, pswfrcmbr, spwfrcmbr, thwfrcmbr, uwfrcmbr, wpwfrcmbr, ydwfrcmbr, ylwfrcmbr

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	48	APPSVR01, DCTLR01, DCTLR02, DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-RB3LBP3, DESKPC-U1K3NAF, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4

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 computers listed below are computers that are marked as "Has ePHI" and are listed in the Computer Identification Worksheet.

The following results were assessed through use of Auditpol:

POLICY	SETTINGS	COMPUTERS
Audit account logon events	Not Enabled	DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-RB3LBP3, DESKPC-U1K3NAF, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4
	Partially Enabled (1 of 4)	DCTLR01, DCTLR02
	Partially Enabled (3 of 4)	APPSVR01, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03
Audit account management	Not Enabled	DESKPC-RB3LBP3
	Partially Enabled (2 of 6)	DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-U1K3NAF, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4
	Partially Enabled (3 of 6)	APPSVR01, DCTLR01, DCTLR02, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03
Audit directory service access	Not Enabled	DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57,

POLICY	SETTINGS	COMPUTERS
		DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-RB3LBP3, DESKPC-U1K3NAF, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4
	Partially Enabled (1 of 4)	APPSVR01, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03
	Partially Enabled (2 of 4)	DCTLR01, DCTLR02
Audit logon events	**Not Enabled**	**DESKPC-RB3LBP3**
	Partially Enabled (1 of 11)	DCTLR01, DCTLR02
	Partially Enabled (5 of 11)	APPSVR01, DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-U1K3NAF, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4
Audit object access	**Not Enabled**	**APPSVR01, DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-RB3LBP3, DESKPC-U1K3NAF, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4**
	Partially Enabled (2 of 14)	DCTLR01, DCTLR02

POLICY	SETTINGS	COMPUTERS
Audit policy change	Not Enabled	DESKPC-RB3LBP3
	Partially Enabled (2 of 6)	APPSVR01, DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-U1K3NAF, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4
	Partially Enabled (3 of 6)	DCTLR01, DCTLR02
Audit privilege use	Not Enabled	APPSVR01, DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-RB3LBP3, DESKPC-U1K3NAF, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4
	Partially Enabled (1 of 3)	DCTLR01, DCTLR02
Audit process tracking	Not Enabled	APPSVR01, DCTLR01, DCTLR02, DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-RB3LBP3, DESKPC-U1K3NAF, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4

POLICY	SETTINGS	COMPUTERS
Audit system events	Not Enabled	DCTLR01, DCTLR02, DESKPC-RB3LBP3
	Partially Enabled (3 of 5)	APPSVR01, DESKPC-09UPSPO, DESKPC-108DSLI, DESKPC-191IJQL, DESKPC-1QSHT11, DESKPC-3IC4R57, DESKPC-4171AR0, DESKPC-4PF2ICP, DESKPC-534MS45, DESKPC-5GTVFB3, DESKPC-7T6GCBK, DESKPC-85BJGJT, DESKPC-ADU1DSQ, DESKPC-AMB2RC8, DESKPC-B9ETSS8, DESKPC-BDJFFLG, DESKPC-E0CVM8B, DESKPC-ELBLDBS, DESKPC-F0M1O27, DESKPC-F6CKERQ, DESKPC-FEQIJCC, DESKPC-FOP1ENA, DESKPC-G0QQU53, DESKPC-H1NN5VD, DESKPC-HN95P9Q, DESKPC-HQJ7BG2, DESKPC-I595F9F, DESKPC-IMMJR2V, DESKPC-LIFRCFU, DESKPC-MA551PF, DESKPC-MVGNQ06, DESKPC-N883DVI, DESKPC-NF6BLBC, DESKPC-P1C4FJP, DESKPC-QFC42PE, DESKPC-U1K3NAF, EXCHSVR01, FILESVR01, HVSVR1, HVSVR2, SQLSVR01, SQLSVR03, WRKSTN10-1, WRKSTN10-2, WRKSTN10-4

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	Yes
Token-based Authentication	Yes
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', and a status of × indicates 'no', or <empty> indicates that a status was not available.

MYCLIENTSNETWORK.COM

COMPUTER NAME	ANTI-VIRUS			ANTI-SPYWARE			FIREWALL		BACKUP	
	NAME	ON	CURRENT	NAME	ON	CURRENT	NAME	ON	NAME	CURRENT
APPSVR01	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DCTLR01	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DCTLR02	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-09UPSPO	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-108DSLI	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-191IJQL	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-1QSHT11	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-35EGQCC										
DESKPC-3IC4R57	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	

COMPUTER NAME	ANTI-VIRUS			ANTI-SPYWARE			FIREWALL		BACKUP	
	NAME	ON	CURRENT	NAME	ON	CURRENT	NAME	ON	NAME	CURRENT
DESKPC-4171AR0	Panda Dome Windows Defender	✓ ✓	✓ ✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-4PF2ICP	Windows Defender	✓	✓	Windows Defender	✓	✗	Windows Firewall	✓	None	
DESKPC-534MS45	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-5GTVFB3	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-7T6GCBK	Windows Defender	✓	✓	Windows Defender	✓	✗	Windows Firewall	✓	None	
DESKPC-85BJGJT	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-ADU1DSQ	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-AMB2RC8	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-B9ETSS8	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-BDJFFLG	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-E0CVM8B	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-ELBLDBS	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-F0M1O27	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-F6CKERQ	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-FEQIJCC	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-FOP1ENA	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-G0QQU53	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-H1NN5VD	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-HN95P9Q	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-HQJ7BG2	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-I595F9F	Windows	✓	✓	Windows	✓	✓	Windows	✓	None	

COMPUTER NAME	ANTI-VIRUS			ANTI-SPYWARE			FIREWALL		BACKUP	
	NAME	ON	CURRENT	NAME	ON	CURRENT	NAME	ON	NAME	CURRENT
	Defender			Defender			Firewall			
DESKPC-IMMJR2V	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-LIFRCFU	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-MA551PF	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-MVGNQ06	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-N883DVI	Windows Defender	✓	✓	Windows Defender	✓	✗	Windows Firewall	✓	None	
DESKPC-NF6BLBC	Windows Defender	✓	✓	Windows Defender	✓	✗	Windows Firewall	✓	None	
DESKPC-P1C4FJP	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-QFC42PE	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-RB3LBP3	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
DESKPC-U1K3NAF	Windows Defender	✓	✓	Windows Defender	✓	✗	Windows Firewall	✓	None	
EXCHSVR01	None			None			Windows Firewall	✓	None	
FILESVR01	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
HVSVR1	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
HVSVR2	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
SQLSVR01	None			None			Windows Firewall	✓	None	
SQLSVR02	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
SQLSVR03	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
WRKSTN10-1	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
WRKSTN10-2	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	
WRKSTN10-4	Windows Defender	✓	✓	Windows Defender	✓	✓	Windows Firewall	✓	None	

Endpoint Security Assessment

Automated detection was unable to be completed on 1 computer. The computers should be investigated to assure proper anti-virus and anti-spyware detection.

- DESKPC-35EGQCC / 176.16.1.179 / Windows 10 Enterprise

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

□ Computer: EXCHSVR01 IP Address: 196.76.48.95
□ Computer: SQLSVR01 IP Address: 176.16.1.17

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

□ Computer: DESKPC-4PF2ICP IP Address: 176.16.1.177 Security Center: Windows Defender
□ Computer: DESKPC-7T6GCBK IP Address: 176.16.1.122 Security Center: Windows Defender
□ Computer: DESKPC-N883DVI IP Address: 176.16.1.124 Security Center: Windows Defender
□ Computer: DESKPC-NF6BLBC IP Address: 176.16.1.117 Security Center: Windows Defender
□ Computer: DESKPC-U1K3NAF IP Address: 176.16.1.175 Security Center: Windows Defender

Security Patch Summary

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

IP ADDRESS	COMPUTER NAME	ISSUE	SCORE	ASSESSMENT
176.16.1.14	**APPSVR01**	**Security Updates, Windows Server 2016**	**Failed (critical)**	**3 security updates are missing.**
		Update Rollups, Windows Server 2016, Windows Server 2019	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2016	Failed (non-critical)	1 update is missing.
176.16.1.12	**DCTLR01**	**Security Updates, Windows Server 2016**	**Failed (critical)**	**1 security update is missing.**
		Update Rollups, Windows Server 2016, Windows Server 2019	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2016	Failed (non-critical)	2 updates are missing.
176.16.1.13	DCTLR02	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2016	Failed (non-critical)	1 update is missing.
176.16.1.169	**DESKPC-09UPSPO**	**Critical Updates**	**Failed (critical)**	**1 critical update is missing.**
		Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.

		Security Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 security update is missing.
		Update Rollups, Windows 10, Windows 10 LTSB, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	3 updates are missing.
		Upgrades	Failed (non-critical)	1 update is missing.
176.16.1.180	DESKPC-191IJQL	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.140	DESKPC-1QSHT11	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.142	DESKPC-3IC4R57	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.173	DESKPC-4171AR0	Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.129	DESKPC-534MS45	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.131	DESKPC-5GTVFB3	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.176	DESKPC-85BJGJT	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.132	**DESKPC-ADU1DSQ**	**Critical Updates**	**Failed (critical)**	**1 critical update is missing.**
		Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.145	**DESKPC-B9ETSS8**	**Critical Updates**	**Failed (critical)**	**1 critical update is missing.**
		Definition Updates, Microsoft Defender	Failed (non-critical)	1 update is missing.

		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.170	DESKPC-BDJFFLG	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.133	DESKPC-ELBLDBS	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.146	DESKPC-FEQIJCC	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.136	DESKPC-FOP1ENA	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.104	DESKPC-H1NN5VD	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.139	DESKPC-HQJ7BG2	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.118, 172.26.144.1	DESKPC-IMMJR2V	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.172	DESKPC-LIFRCFU	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.144, 192.168.217.193	DESKPC-MA551PF	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.100, 172.31.48.1	DESKPC-MVGNQ06	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.114	DESKPC-P1C4FJP	Definition Updates, Microsoft Defender	Failed (non-critical)	1 update is missing.

IP ADDRESS	COMPUTER NAME	ISSUE	SCORE	ASSESSMENT
		Antivirus		
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.182	DESKPC-QFC42PE	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.181	DESKPC-RB3LBP3	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10 LTSB	Failed (non-critical)	2 updates are missing.
196.76.48.95, 176.16.1.15	EXCHSVR01	Definition Updates, MS Security Essentials	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2012 R2	Failed (non-critical)	1 update is missing.
176.16.1.16	FILESVR01	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
196.76.50.35, 196.76.70.176, 176.16.1.148, 176.16.1.7, 176.16.1.101	HVSVR1	Security Updates	Failed (non-critical)	1 security update is missing.
		Security Updates, Windows Server, version 1903 and later	Failed (non-critical)	1 security update is missing.
		Updates, Windows Server, version 1903 and later	Failed (non-critical)	2 updates are missing.
196.76.0.2, 176.16.1.147, 176.16.1.8, 176.16.1.110, 176.16.1.109	HVSVR2	Security Updates	Failed (non-critical)	1 security update is missing.
		Security Updates, Windows Server, version 1903 and later	Failed (non-critical)	1 security update is missing.
		Updates, Windows Server, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.17	SQLSVR01	Definition Updates, MS Security Essentials	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2012 R2	Failed (non-critical)	1 update is missing.
176.16.1.107	SQLSVR03	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
		Microsoft SQL Server 2019, Security Updates	Failed (non-critical)	1 security update is missing.
		Microsoft SQL Server 2019, Updates	Failed (non-critical)	1 update is missing.
		Security Updates	Failed (non-critical)	1 security update is missing.
		Security Updates, Windows Server 2019	Failed (non-critical)	1 security update is missing.
		Update Rollups, Windows	Failed (non-critical)	1 update is missing.

IP ADDRESS	COMPUTER NAME	ISSUE	SCORE	ASSESSMENT
		Server 2016, Windows Server 2019		
		Updates, Windows Server 2019	Failed (non-critical)	2 updates are missing.
176.16.1.138	WRKSTN10-1	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.143	WRKSTN10-2	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.149	WRKSTN10-4	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.125	DESKPC-108DSLI	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.177	DESKPC-4PF2ICP	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.122	DESKPC-7T6GCBK	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.106	DESKPC-E0CVM8B	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.174	DESKPC-F0M1O27	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.171	DESKPC-F6CKERQ	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.108	DESKPC-G0QQU53	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.193	DESKPC-HN95P9Q	Definition Updates,	Failed (non-critical)	1 update is missing.

		Microsoft Defender Antivirus		
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	2 updates are missing.
176.16.1.102	DESKPC-I595F9F	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.124	**DESKPC-N883DVI**	**Critical Updates**	**Failed (critical)**	**1 critical update is missing.**
		Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.117	DESKPC-NF6BLBC	Definition Updates, Microsoft Defender Antivirus	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.

Security Patch Assessment

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.

Copiers and Multi-function Printers

Copiers and/or Multi-function Printers are in use, but have not been documented in the On-Site Survey.

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.

5.3 - Disk Encryption Analysis of ePHI Computers

§164.312(a)(2)(iv): Encryption and Decryption - Implement a mechanism to encrypt and decrypt electronic protected health information.

Computer Disk Encryption

A disk encryption analysis has been performed on accessible computer endpoints available on the network during the assessment process. To review the results of this analysis, please refer to the Disk Encryption report.

USB Drive Use

No USB drives found

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:	Sophos XG 115

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): Protection from Malicious Software - Procedures for guarding against, detecting, and reporting malicious software.

The external firewall does have Malware Filter; however, the subscription is not current.

6.3 - External Vulnerability Scan

§164.308(a)(5)(ii)(b): Protection from Malicious Software - 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 Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	FALSE	HIGHEST CVSS

HOST	OPEN PORTS	HIGH	MED	LOW	FALSE	HIGHEST CVSS
97.68.119.142 (97-68-119-142-static.atl.earthlink.net)	2	0	1	1	0	4.3
Total: 1	2	0	1	1	0	4.3

The following high and medium risk issues were detected. Further details and low risk issues can be found in the External Vulnerability Scan Detail report. Issues that have been investigated and marked as either false positives or with compensating controls are marked non-issues with entries in the Security Exception Worksheet.

97.68.119.142

CVSS	SEVERITY	ISSUE	MITIGATED
4.3	**Medium**	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.117274) Port: 33089/tcp	No

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
No entries.		

8 - Wireless

8.1 - Access Authorization

§164.308(a)(4)(ii)(B): Access Authorization - 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.

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.

We do not employ a wireless network for employees and vendors.

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).

We do not provide wireless to employees or vendors.

9 - Business Associates

9.1 - Business Associate Agreements with Service Providers

§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.

Our organization does not have any Business Associates that meet the requirements of the 2013 HIPAA Omnibus Final Rule. This compliance requirement is not applicable.

9.2 - Cloud Servers and Data Centers

§164.308(a)(7)(ii)(a): Data Backup Plan - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. §164.308(a)(7)(ii)(b): Establish (and implement as needed) procedures to restore any loss of data.

9.2.1 - Cloud Servers

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

Contact Information:	Haltan Data Center Services, Inc. Contact: Joseph Wingmar Email: jwingmar@hdcci.net

9.2.2 - Data Center

We use a data center.

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

9.3 - eFax Service

9.3.1 - Send Faxes

We use an eFax Service to send faxes.

We do not have a Business Associate Agreement with the eFax Service.

9.3.2 - Receive Faxes

We use an eFax Service to receive faxes.

We do not have a Business Associate Agreement with the eFax Service.

9.4 - 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	MITIGATED
AnyDesk	APPSVR01		Yes	No	No
AnyDesk	DCTLR01		Yes	No	No
AnyDesk	DCTLR02		Yes	No	No
AnyDesk	DESKPC-09UPSPO		Yes	No	No
AnyDesk	DESKPC-191IJQL		Yes	No	No
AnyDesk	DESKPC-4171AR0		Yes	No	No
AnyDesk	DESKPC-4PF2ICP		Yes	No	No
AnyDesk	DESKPC-534MS45		Yes	No	No
AnyDesk	DESKPC-7T6GCBK		Yes	No	No
AnyDesk	DESKPC-85BJGJT		Yes	No	No
AnyDesk	DESKPC-AMB2RC8		Yes	No	No
AnyDesk	DESKPC-BDJFFLG		Yes	No	No
AnyDesk	DESKPC-E0CVM8B		Yes	No	No
AnyDesk	DESKPC-F0M1O27		Yes	No	No
AnyDesk	DESKPC-F6CKERQ		Yes	No	No
AnyDesk	DESKPC-G0QQU53		Yes	No	No
AnyDesk	DESKPC-H1NN5VD		Yes	No	No
AnyDesk	DESKPC-HN95P9Q		Yes	No	No

SERVICE	COMPUTER	EXPLANATION OF USE	EPHI RISK	BA AGREEMENT	MITIGATED
AnyDesk	DESKPC-I595F9F		Yes	No	No
AnyDesk	DESKPC-IMMJR2V		Yes	No	No
AnyDesk	DESKPC-LIFRCFU		Yes	No	No
AnyDesk	DESKPC-MA551PF		Yes	No	No
AnyDesk	DESKPC-MVGNQ06		Yes	No	No
AnyDesk	DESKPC-N883DVI		Yes	No	No
AnyDesk	DESKPC-NF6BLBC		Yes	No	No
AnyDesk	DESKPC-P1C4FJP		Yes	No	No
AnyDesk	DESKPC-QFC42PE		Yes	No	No
AnyDesk	DESKPC-RB3LBP3		Yes	No	No
AnyDesk	DESKPC-U1K3NAF		Yes	No	No
AnyDesk	EXCHSVR01		Yes	No	No
AnyDesk	FILESVR01		Yes	No	No
AnyDesk	SQLSVR01		Yes	No	No
AnyDesk	SQLSVR02		Yes	No	No
AnyDesk	SQLSVR03		Yes	No	No
AnyDesk	WRKSTN10-1		Yes	No	No
AnyDesk	WRKSTN10-2		Yes	No	No
AnyDesk	WRKSTN10-4		Yes	No	No

9.5 - 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.

10 - Administrative, Physical, and Technical Safeguard Policies and Procedures

10.1 - Sanction Policy

HIPAA Section(s): §164.308(a)(1)(ii)(C): Sanction policy - Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

Our organization has implemented a Sanction policy.

Exhibits:

- Covered Entity Sanction Policy.pdf

Comments:

No comments available.

10.2 - Access Policy

HIPAA Section(s): §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.

Our organization has implemented an Access policy.

Exhibits:

- Covered Entity Access Policy.pdf

Comments:

No comments available.

10.3 - Security Incident Response and Reporting Plan

HIPAA Section(s): §164.308(a)(6)(i): Security incident procedures - Implement policies and procedures to address security incidents.

Our organization has implemented Security Incident and Reporting Plan policies and procedures.

Exhibits:

- Covered Entity Security Incident Response and Reporting Plan.pdf

Comments:

No comments available.

10.4 - Disaster Recovery Plan

HIPAA Section(s): §164.308(a)(7)(i): Contingency plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

10.5 - Emergency Mode Operations Plan

HIPAA Section(s): §164.308(a)(7)(i): Contingency plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Our organization has implemented Emergency Mode Operations Plan policies and procedures.

Exhibits:

- Covered Entity Emergency Mode Operations Plan.pdf

Comments:

No comments available.

10.6 - Contingency Plan

HIPAA Section(s): §164.308(a)(7)(i): Contingency plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

10.7 - Application and Data Criticality Analysis

HIPAA Section(s): §164.308(a)(7)(i): Contingency plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

Our organization has implemented Application and Data Criticality Analysis policies and procedures.

Exhibits:

- Covered Entity Application and Data Criticality Analysis.pdf

Comments:

No comments available.

10.8 - Evaluation

HIPAA Section(s): §164.308(a)(8): Evaluation - Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

10.9 - Business Associates Agreement

HIPAA Section(s): §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.

Our organization has implemented Business Associates Agreement policies and procedures.

Exhibits:

- Covered Entity Sample Business Associates Agreement.pdf

Comments:

No comments available.

10.10 - Facility Security Plan

HIPAA Section(s): §164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Our organization has implemented Facility Security Plan policies and procedures.

Exhibits:

- Covered Entity Facility Security Plan.pdf

Comments:

No comments available.

10.11 - Access Control and Validation Procedure

HIPAA Section(s): §164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Our organization has implemented Access Control and Validation Procedure policies and procedures.

Exhibits:

- Covered Entity Access Control and Validation Procedure.pdf

Comments:

No comments available.

10.12 - Facility Access Control Maintenance Records

HIPAA Section(s): §164.310(a)(1): Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

10.13 - Workstation Use Policy

HIPAA Section(s): §164.310(b): Workstation use - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

Our organization has implemented a Workstation Use Policy.

Exhibits:

- Covered Entity Workstation Use Policy.pdf

Comments:

No comments available.

10.14 - Workstation Security

HIPAA Section(s): §164.310(c): Workstation security - Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Our organization has implemented Workstation Security policies and procedures.

Exhibits:

- Covered Entity Workstation Security Policy.pdf

Comments:

No comments available.

10.15 - Media Disposal Policy

HIPAA Section(s): §164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Our organization has implemented a Media Disposal Policy.

Exhibits:

- Covered Entity Media Disposal Policy.pdf

Comments:

No comments available.

10.16 - Media Re-use Procedure

HIPAA Section(s): §164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

10.17 - Media Accountability Procedure

HIPAA Section(s): §164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Our organization has implemented a Media Accountability Procedure.

Exhibits:

- Covered Entity Media Accountability Procedure.pdf

Comments:

No comments available.

10.18 - Data Backup and Storage Procedure

HIPAA Section(s): §164.310(d)(1): Device and media controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

10.19 - Emergency Access Procedure

HIPAA Section(s): §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).

Our organization has implemented an Emergency Access Procedure.

Exhibits:

- Covered Entity Emergency Access Procedure.pdf

Comments:

No comments available.

10.20 - Integrity of Data Procedure

HIPAA Section(s): §164.312(c)(1): Integrity - Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

10.21 - Integrity Control Procedure

HIPAA Section(s): §164.312(e)(1): Transmission Security - Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Our organization has implemented an Integrity Control Procedure.

Exhibits:

- Covered Entity Integrity Control Procedure.pdf

Comments:

No comments available.

10.22 - ePHI Transmission Encryption Procedure

HIPAA Section(s): §164.312(e)(1): Transmission Security - Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

11 - Privacy Rule

11.1 - Health Care Provider - Notice of Privacy Practices

§164.520: Notice of Privacy Practices for PHI, **§164.520(a)(1):** Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

11.1.1 - Notice of Privacy Practices Policy

§164.520: Notice of Privacy Practices for PHI, **§164.520(a)(1):** Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

Our organization has implemented Notice of Privacy Practices policies and procedures.

Exhibits:

- Notice of Privacy Practices Policy for Medical Providers.pdf

Comments:

No comments available.

11.1.2 - Notice of Privacy Practices - Required Wording

§164.520: Notice of Privacy Practices for PHI, **§164.520(a)(1):** Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

Our organization has implemented Notice of Privacy Practices - Required Wording policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.1.3 - Notice of Privacy Practices - Given to All New Patients

§164.520: Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.

Our organization has implemented Notice of Privacy Practices - Given to All New Patients policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.1.4 - Notice of Privacy Practices - Acknowledgement Received from All New Patients

§164.520: Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.

Our organization has implemented Notice of Privacy Practices - Acknowledgement Received from All New Patients policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.1.5 - Notice of Privacy Practices - Available Upon Request

§164.520: Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.

Our organization has implemented Notice of Privacy Practices - Available Upon Request policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.1.6 - Notice of Privacy Practices - Posted in Patient Area

§164.520: Notice of Privacy Practices for PHI, **§164.520(c)(2) (iii)(B):** A covered health care provider that has a direct treatment relationship with an individual must: Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice.

Our organization has implemented Notice of Privacy Practices - Posted in Patient Area policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.1.7 - Notice of Privacy Practices - Prominently Displayed on Website

§164.520: Notice of Privacy Practices for PHI, **§164.520(c)(2) (iii)(B):** A covered health care provider that has a direct treatment relationship with an individual must: Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.2 - Group Healthcare Plans - Notice of Privacy Practices

§164.520: Notice of Privacy Practices for protected health information

11.2.1 - Providing and Displaying Notice of Privacy Practices

§164.520: Notice of Privacy Practices for protected health information

The organization is not a Group Healthcare Plan Provider.

11.2.2 - Notice of Privacy Practices Provided to All New Members

§164.520: Notice of Privacy Practices for protected health information

The organization is not a Group Healthcare Plan Provider.

11.2.3 - Notice of Privacy Practices Prominently Displayed on Website

§164.520: Notice of Privacy Practices for protected health information - Uses and disclosures consistent with notice.

The organization is not a Group Healthcare Plan Provider.

11.2.4 - Notice of Privacy Practices - Workforce Training

§164.520: Notice of Privacy Practices for protected health information

The organization is not a Group Healthcare Plan Provider.

11.3 - Patient's Right to Access Records

§164.524(b)(1) The covered entity must permit an individual to request access to review or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

§164.524(c)(3) If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

11.3.1 - Written Patient's Right to Access Records Policy

§164.524: Access of individuals to protected health information.

Our organization has implemented Written Patient's Right to Access Records policies and procedures.

Exhibits:

- Patient’s Rights to Access Records Policy.pdf

Comments:

No comments available.

11.3.2 - Fees for Medical Records Consistent with HIPAA and Other Regulations

§164.524: Access of Individuals to PHI, §164.524(b)(4) If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of: (i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual; (ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and (iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.

Our organization has implemented Patient's Right to Access Records - Fees policies and procedures consistent with HIPAA and other regulations.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.3.3 - Patient's Rights to Access Records - Deadline

§164.524: Access of individuals to protected health information.

Our organization has implemented Patient's Right to Access Records - Deadline policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.3.4 - Patient's Rights to Access Mental Health Records

§164.524: Access of individuals to protected health information.

Our organization has implemented Patient's Right to Access Mental Health Records policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.3.5 - Patient's Rights to Access Records - What to Provide

§164.524: Access of individuals to protected health information.

Our organization has implemented Patient's Right to Access Records - What to Provide policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.3.6 - Patient's Rights to Access Records - Deceased Individuals

§164.524: Access of individuals to protected health information.

Our organization has implemented Patient's Right to Access Records - Deceased Individuals policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.4 - Law Enforcement, Court Orders, and Subpoenas

§164.512: Uses and Disclosure - Standard: Disclosures for judicial and administrative proceedings.

11.4.1 - Law Enforcement, Court Orders, and Subpoenas Policy

§164.512: Uses and Disclosure - Standard: Disclosures for judicial and administrative proceedings.

Our organization has implemented Law Enforcement, Court Orders, and Subpoenas policies and procedures.

Exhibits:

- Law Enforcement - Court Orders and Subpoenas Policy.pdf

Comments:

No comments available.

11.4.2 - Law Enforcement, Court Orders, and Subpoenas Policy - Workforce Training

§164.512: Uses and Disclosure - Standard: Disclosures for judicial and administrative proceedings.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.5 - Marketing

§164.501: Marketing: Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

§164.508: Uses and disclosures for which an authorization is required, **§164.508(a)(3):** Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing.

11.5.1 - HIPAA-related Marketing Policy

§164.508: Uses and disclosures for which an authorization is required, **§164.508(a)(3):** Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing.

Our organization has implemented HIPAA-related Marketing policies and procedures.

Exhibits:

- Marketing Policy.pdf

Comments:

No comments available.

11.5.2 - HIPAA-related Marketing Policy - Workforce Training

§164.508: Uses and disclosures for which an authorization is required, **§164.508(a)(3):** Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.6 - Minimum Necessary Access

§164.502(b) - Uses and disclosures of protected health information - Minimum necessary,

§164.514(d) - Other requirements relating to uses and disclosures of protected health information - Minimum necessary use of electronic personal health information.

11.6.1 - Minimum Necessary Access Policy

§164.502(b) - Uses and disclosures of protected health information - Minimum necessary,

§164.514(d) - Other requirements relating to uses and disclosures of protected health information - Minimum necessary use of electronic personal health information.

Our organization has implemented Minimum Necessary Access policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.6.2 - Minimum Necessary Access - Workforce Training

§164.502(e): Uses and disclosures of protected health information,

§164.504(e): Uses and disclosures - organizational requirements,

§164.532(d): Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.6.3 - Minimum Necessary Access - Internal Auditing

§164.502(e): Uses and disclosures of protected health information,

§164.504(e): Uses and disclosures - organizational requirements,

§164.532(d): Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.

Our organization has implemented Minimum Necessary Access - Internal Auditing policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.7 - Confidential Communications

§164.522(b): Rights to request privacy protection for protected health information - Confidential communications requirements.

11.7.1 - Confidential Communications - Policy

§164.522(b): Rights to request privacy protection for protected health information - Confidential communications requirements.

Our organization has implemented Confidential Communications policies and procedures.

Exhibits:

- Confidential Communications Policy.pdf

Comments:

No comments available.

11.7.2 - Confidential Communications - Workforce Training

§164.522(b): Rights to request privacy protection for protected health information - Confidential communications requirements.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.7.3 - Confidential Communications - Documentation

§164.522(b): Rights to request privacy protection for protected health information - Confidential communications requirements.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.7.4 - Confidential Communications - Systems/Processes

§164.522(b): Rights to request privacy protection for protected health information - Confidential communications requirements.

Our organization has implemented Confidential Communications - Systems/Processes policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.8 - Business Associates

§164.502(e): Uses and disclosures of protected health information, **§164.504(e):** Uses and disclosures - organizational requirements, **§164.532(d):** Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.

11.8.1 - Policy and Procedures for Business Associates

§164.502(e): Uses and disclosures of protected health information, **§164.504(e):** Uses and disclosures - organizational requirements, **§164.532(d):** Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.

Our organization has implemented policies and procedures for Business Associates.

Exhibits:

- Covered Entity Sample Business Associates Agreement.pdf

Comments:

No comments available.

11.8.2 - Workforce Training on the Management of Business Associates

§164.502(e): Uses and disclosures of protected health information, **§164.504(e):** Uses and disclosures - organizational requirements, **§164.532(d):** Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.

Our organization has implemented Workforce Training on the Management of Business Associates policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.8.3 - Business Associate Agreements with Vendors and Contractors

§164.502(e): Uses and disclosures of protected health information, **§164.504(e):** Uses and disclosures - organizational requirements, **§164.532(d):** Transition provisions - Standard: Effect of prior contracts or other arrangements with business associates, and (e) - Implementation specification: Deemed compliance.

Our organization has implemented Business Associate Agreements with Vendors and Contractors policies and procedures.

Exhibits:

- Covered Entity Sample Business Associates Agreement.pdf

Comments:

No comments available.

11.9 - Authorizations for Uses and Disclosures

§164.508: Uses and disclosures requiring an opportunity for the individual to agree or to object - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.

11.9.1 - Authorizations for Uses and Disclosures Policy

§164.508: Uses and disclosures requiring an opportunity for the individual to agree or to object - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.

The organization has not implemented this policy requirement.

11.10 - Uses and Disclosures - Emergencies and Disasters

§164.510(b): Standard: Uses and disclosures for involvement in the individual's care and notification purposes -

11.10.1 - Uses and Disclosures - Emergencies and Disasters Policy

§164.510(b)(4): Limited uses and disclosures when the individual is not present - Uses and disclosures for disaster relief purposes.

Our organization has implemented Uses and Disclosures - Emergencies and Disasters policies and procedures.

Exhibits:

- Covered Entity Emergency Access Procedure.pdf

Comments:

No comments available.

11.10.2 - Uses and Disclosures - Emergencies and Disasters - Workforce Training

§164.510(b): Uses and disclosures for which authorization is required - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

11.11 - Uses and Disclosures - Mental and Behavioral Health, including Opioid Overdose

§164.510(b): Standard: Uses and disclosures for involvement in the individual's care and notification purposes - **§164.510(b)(3)** - Limited uses and disclosures when the individual is not present. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

11.11.1 - Uses and Disclosures - Mental and Behavioral Health, including Opioid Overdose Policy

§164.510(b): Uses and disclosures for which authorization is required - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.

Our organization has implemented Uses and Disclosures - Mental and Behavioral Health, including Opioid Overdose policies and procedures.

Exhibits:

- Uses and Disclosures Policy – Mental and Behavioral Health Policy.pdf

Comments:

No comments available.

11.11.2 - Uses and Disclosures - Mental and Behavioral Health, including Opioid Overdose - Workforce Training

§164.510(b): Uses and disclosures for which authorization is required - Standard: Uses and disclosures for involvement in the individual's care and notification purposes.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

12 - Breach Notification Rule

12.1 - Breach Complaint and Determination

§164.414(a),

§164.530(i): Administrative Requirements §164.530(i)(1) A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. §164.530(i)(2)(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart.

12.1.1 - Breach Complaint and Determination Policy

§164.414: Administrative requirements and burden of proof.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

12.1.2 - Breach Complaint and Determination - Workforce Training

§164.530(b): Administrative requirements - Standard: Training and Implementation specifications: Training.

Our organization has implemented Breach Complaint and Determination - Workforce Training policies and procedures.

Exhibits:

No exhibits available.

Comments:

No comments available.

12.2 - Breach Risk Assessment

§164.402 - Definitions Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

§164.530(i): Administrative Requirements §164.530(i)(1) A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. §164.530(i)(2)(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart.

12.2.1 - Breach Risk Assessment Policy

§164.414: Administrative requirements and burden of proof.

Our organization has implemented Breach Risk Assessment policies and procedures.

Exhibits:

- Breach Notification Rule Policy – Notices – Other Regulatory Compliance – Insurance Compliance.pdf

Comments:

No comments available.

12.2.2 - Breach Risk Assessment - Workforce Training

§164.530(b): Administrative requirements - Standard: Training and Implementation specifications: Training.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

12.3 - Individual Notification

§164.404: Notice to Individuals - §164.404 (a) A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.

164.404(b) Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.

12.3.1 - Breach Individual Notification Policy

§164.404: Notification to individuals - Standard: General rule for unsecured protected health information breach notification.

Our organization has implemented Breach Individual Notification policies and procedures.

Exhibits:

- Breach Notification Rule Policy – Notices – Other Regulatory Compliance – Insurance Compliance.pdf

Comments:

No comments available.

12.3.2 - Breach Individual Notification - Workforce Training

§164.530(b): Administrative requirements - Standard: Training and Implementation specifications: Training.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.

12.4 - Regulatory Reporting

§164.408: Notification to the Secretary - §164.408(a) A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary (b) For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site. (c) For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.

12.4.1 - Breach Reporting Policy

§164.408: Notification to the Secretary - Standard: A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in, **§164.404(a)(2)** notify the Secretary of HHS.

Our organization has implemented Breach Reporting policies and procedures.

Exhibits:

- Breach Notification Rule Policy – Notices – Other Regulatory Compliance – Insurance Compliance.pdf

Comments:

No comments available.

12.4.2 - Breach Reporting - Workforce Training

§164.530(b): Administrative requirements - Standard: Training and Implementation specifications: Training.

Our organization has not implemented this policy requirement.

Exhibits:

No exhibits available.

Comments:

No comments available.