kypher
01101011
Encryption, Compliance, One Application

Security Risk Assessment

Murdoch Vision Care

1010 Chestnut Blvd.
Suite 101
St. Louis, MO 63101

Beginning July 8th 2016 through July 15th 2016 Kypher, LLC performed a Security Risk Assessment for Murdoch Vision Care for the calendar year 2016.

This risk assessment includes the following physicians:

Dr. Arthur Stevenson

Dr. Melissa Roberts

Dr. Keith Wilcoxen

Enclosed, please find the results of the Security Risk Assessment. The results are formatted using the CMS risk assessment tool.

Melony Tanko
President/Co-founder
Kypher

08/11/2016

To: Randall Murdoch (Murdoch Vision Care)

From: Melony Tanko, President – Kypher LLC

Re: Security Risk Assessment – 2016

Date: August 11nd, 2016

Introduction

Beginning July 8th, 2016 through July15th 2016, Kypher LLC ("Kypher") conducted a comprehensive security risk assessment of Murdoch Vision Care Associates (Murdoch Vision Care).

The security risk assessment was broken up into three main areas of safeguards: Physical, Technical and Administrative. Several members of the Kypher team visited and gathered information ranging from cataloging, deployment and positioning of computer equipment to staff workflows and practice policies and how they affect patient health information ("PHI") and ePHI (electronic patient health information) compliance. The Kypher Team was comprised of IT and compliance security specialists skilled in assessing all physical, technical and administrative aspects of the business operations of Murdoch Vision Care.

This Memorandum ("Memorandum") contains a description of our findings as well as recommendations to strengthen and bolster the security of Murdoch Vision Care's business operations.

The following section contains the security risk scorecard. Within this section risk issues will be discussed covering *physical* security, *technical* security, and *administrative* security. The rated status of each item will be expressed in the following categories and color codes:

Critical – Immediate fix is needed!

High – Fix as soon as possible

Medium – Should be fixed within the next 3 months

Low – Should be fixed within the next 6-12 months

Passed – No action needed

Risks & Findings Scorecard

This scorecard shows the overall health and risk severity levels for each category. This is determined by the highest severity issue found per category and its associated risk.

The severity always represents the highest issue level found in a category, the value is not calculated.

Consolidated Scorecard	Risk Potential	Assesment Finding
***PHYSICAL* SECURITY Risks and Safeguards**		
PHI and ePHI removal from decommissioned hardware	High	*Passed -*
MVC works with IT vendor and EPS for proper destruction of any decommissioned hardware containing ePHI.		*Documentation of this process should be added to the compliance plan.*
Monitor positioning to prevent unauthorized viewing of PHI	Low	*Passed*
MVC is aware of monitor positioning for privacy and attempt to follow this. There is a possibility to see a workstation screen from the far right of the front desk or behind the wall separating the front desk and patient waiting area but the area layout makes this unlikely/difficult.		*Use of screen protectors would elimanate any reasonable possiblity of unauthorized viewing.*
All areas that contain ePHI/PHI are not secured	High	*Action needed*
Consider placing locks on the doors that contain the server as well as the room that contains the network hardware. If locked rooms are not practical consider lockable cabinets/enclosures.		
Business location is secured out of regular business hours	High	*Passed*
Both front and back doors are secured with lock and key and an alarm system is used to detect unauthorized entry. A video camera is present but recording is not enabled making use of video surveillance less effective.		*– but recommend that recording of video camera be implemented.*
No facility access policy	High	*Action needed*
Create a facility access policy (that you make a part of the larger HIPAA compliance plan). This policy should include prodcedures to re-key locks in the case of employee termination. Also include provisions about who has access to the facility in case of an emergency.		
No record of devices that leave the office	Low	*Action needed*
Create a policy section in the HIPAA compliance plan that speaks to having a log to track hardware devices(containing ePHI).		

Consolidated Scorecard	Risk Potential	Assesment Finding
No workstation/endpoint policy in place	Medium	*Action needed*
Create a workstation best uses policy(make it a part of the HIPAA compliance plan)		
No data destruction plan	Medium	*Action needed*
Develop a data destruction plan that includes provisions for who will be destroying the data and what proof will be provided		
No full asset inventory of ePHI bearing technology	Low	*Action taken*
Kypher is assisting in creating a full and up to data asset list as part of the assessment		
***ADMINISTRATIVE* SECURITY Risks and Safeguards**		
No HIPAA compliance document exists	High	*Action Needed*
Create a full HIPAA compliance plan. Update the policy each year to include any changes in technology, workflow, or security. Make sure all sub plans align with each other.		
No formal documented employee handbook	Medium	*Action Needed*
Create an employee hand book and train the staff. Include sections regarding adherence to security requirements		
No disaster recovery plan	High	*Action Needed*
Establish a disaster recovery plan and include it in the final HIPAA compliance plan. Consider what emergencis or disasters could do the integrity of your ePHI data. Test a simulated disater and recover at least once a year. Include provisions about the existing on-site backup and cloud backup. Prioritize the data that would need to be recovered and map out a clear path to that recovery.		
No facility security plan	High	*Action Needed*
Create a facility security plan and include it in the final HIPAA compliance plan.		
No training of staff on compliance plan	High	*Action Needed*
Train users annually on compliance plan and have them sign off upon completion. Make sure all policies align together.		
Background checks of employees	Medium	*Passed*
Murdoch Vision Care performs background checks on employees as needed.		
Practice has identified vendors with ePHI access	Medium	*Passed -*
Document the list and execute business associate agreements(BAA) with members on the list. A BAA document is in place for Kypher		*Some additional action recommended*
Security Risk Assessment(SRA)	High	*Passed*
The practice is performing its annual SRA to understand and mitigate HIPAA threats		

Consolidated Scorecard	Risk Potential	Assesment Finding
Identify a HIPAA compliance officer	Medium	*Passed*
The practice has identified a compliance officer and security point of contact(Randall Murdoch). The staff is aware to report breach or other security issues to the Randall.		
No Business Associate Agreement	High	*Action Needed*
Create a standard business associate agreement for the practice. Have each vendor, contractor and any other business associate handling ePHI/PHI sign the agreement. Update agreement annually to account for technical, workflow or any other practice changes. Make sure the agreement meets the recommendation for safeguaring ePHI(including terms and conditions for the business associate to implement security safeguards to protect ePHI)		
No written procedures for handling new user requests or updates	Low	*Action Needed*
Establish a documented workkflow for handling new user requests, changes or removals as part of the employee handbook.. The process should include logging of the justification for the account maintenance.		
No definition of ePHI access rules	Medium	*Action Needed*
Consider adding an access definition to the HIPAA conpliance plan describing the rule of least priviledge as it relates to access (users are granted only the needed access for their job duties and nothing more). Both a policy and training on proper use of ePHI/PHI should be a part of your regular annual HIPAA review.		
No policy regarting ePHI access by outside users/vendors	Low	*Action needed*
Create an access request form to be used by external users/vendors that includes details about the limits and HIPAA obligations for accessing practice ePHI. Make sure access is limited. Have each requester sign the form indicating their acceptance of the responsibilities regarding care and handling of ePHI.		
No Security incident response plan	High	*Action needed*
Create a security incident response plan as part of your HIPAA compliance plan document. This should include the person to be contacted in the event of a security incident or breach, along with what information is to be provided. Test the incident responce plan annually. Create example scenarios to be used in the annual tests		
No auditing or access reviews	Medium	*Action Needed*
Enable auditing of ePHI access and set a process for periodic review of audit data.		
***TECHNICAL* SECURITY Risks and Safeguards**		

Consolidated Scorecard	Risk Potential	Assesment Finding
ISP provided router has administrative and Wifi passwords printed on the external lable	**High-critical**	*Action Needed*
Change the default administrator and Wifi passwords from the values printed on the external device label. The password should be at least 8 characters in length and contain letters, numbers and special characters. The gateway IP had been changed from what was displayed on the label but was easily obtained through access to the Wifi network using the password available on the label.		
Generic, Shared Logins are used	High	*Action Needed*
Each member of the staff should be required to have(and use) their own unique account for access of ePHI. Accounts could be grouped into Windows Global Groups for the granting of role based privileges such as access to Office Mate. Don't just give full access to each individual user. *This would help clarify an audit trail for ePHI usage and maintenance. Individual IDs should have a password expiration policy requiring change every 90 days or less*		
No Anti-Malware software is installed and no regular scans are performed	High	*Action Needed*
During our review scans reveiled a number of PCs contained trojans and PUPs(potentially unwanted programs). Consider obtaining AM software and perform regular scans of all PCs.		
No messaging or email encryption	High	*Action Needed*
Consider a messaging and email solution that would encrypt and protect your outbound messages as well as inbound protection from viruses/malware/span and targeted threats.		
SQLServer cloud backups incomplete	High	*Action Needed*
At the time of the site visit it was determined that the DDB Cloud backups for sqlserver lacked a recent full backup. Randall was notified and indicated he would perform a full backup to resolve.		
Unattended monitor screens lock after timeout.	High	*Passed -*
Common, generic user IDs are in an active directory policy that enforces timeout and screen lock. Consider using unique IDs within role based global groups.		*Unique, assigned user IDs operating within role based global groups would provide better security, control and audit of HIPAA data resources.*
Backup for critical system data	High	*Passed*

Consolidated Scorecard	Risk Potential	Assesment Finding
MVC performs backups of their server data both locally and to the cloud using backup clients which provide for encryption of backup data.		
Active Directory control of users and groups	High	Passed
MVC has implemented Windows Active Directory for domain usesrs and groups. Should move to uniquely assigned IDs within role based groups for better protection of ePHI		*Additional Action recommended*
No endpoint or OS level encryption	High	*Action Needed*
Use an endpoint encryption provider for all machines containing ePHI. Require strong passwords to protect this data.		
No data security when ePHI leaves the office	High	*Review Needed*
Consider encryption data prior to leaving the office for any reason...including removable storage.		
No emergency access to ePHI	High	*Review Needed*
Use disaster recovery testing to set up an emergency access plan that will allow for minimal access to necessary data...as needed to see patients.		
No Audit policies in place	High	*Review Needed*
Consider adding built in Windows domain audit control including object and logon/logoff access auditing. Retain and backup audit logs and keep them indefinitely.		
No next generation firewall	High	*Action Needed*
Firewall in place now is the ISP default and should only be used in bridge mode(as a modem). A newer next generation firewall should be used to protect inbound and outbound traffic. This firewall should include intrusion detection and prevention.		

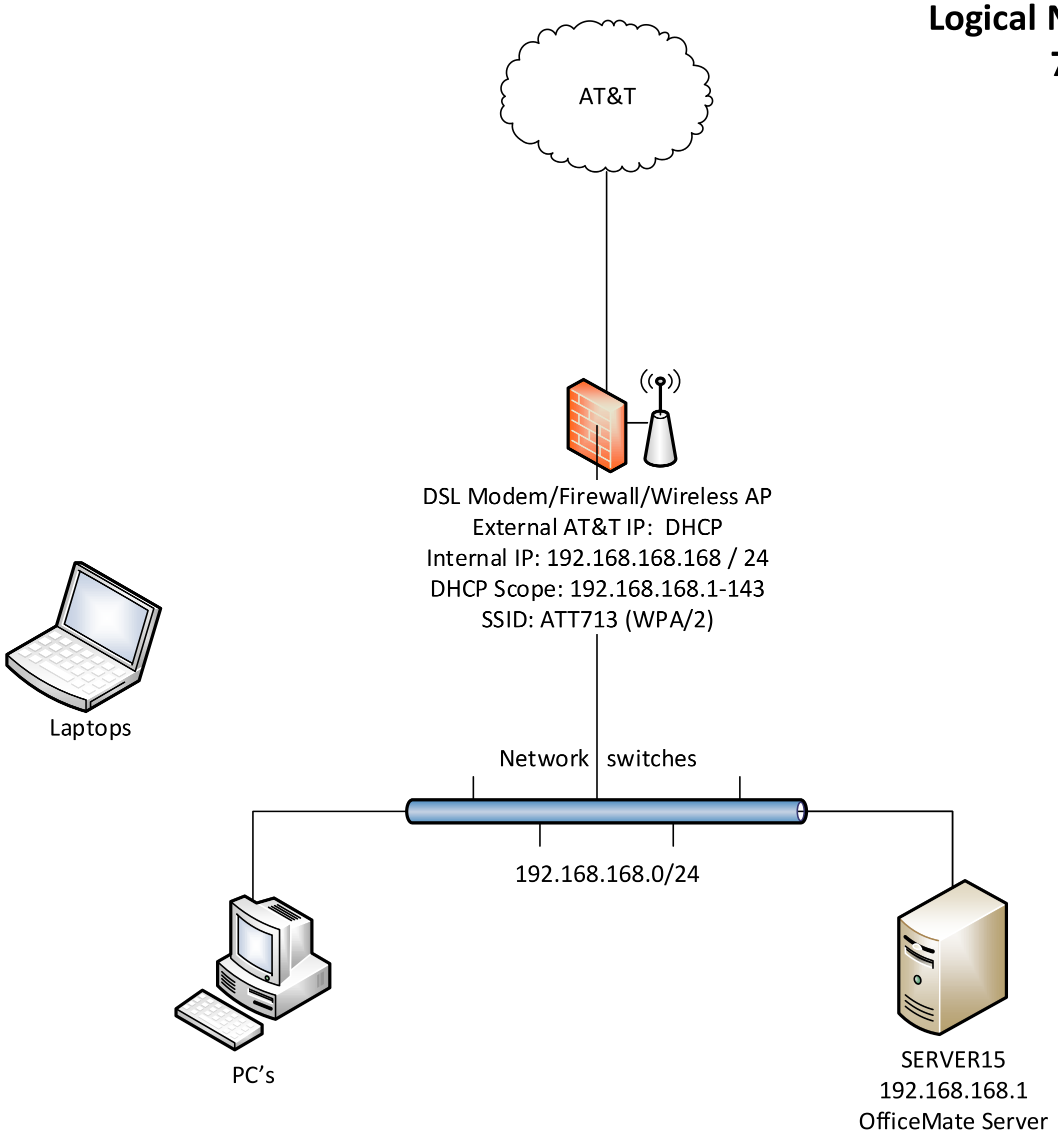
Conclusion

Kypher's review of the physical, technical and administrative security aspects of Murdoch Vision Care's business operations illustrated that Murdoch Vision Care takes seriously potential threats to its security by taking proactive steps to avoid a security incident. This Memorandum highlights the physical, technical and administrative security measures that Murdoch Vision Care has implemented to bolster the security of its business operations. In addition, this Memorandum includes recommendations, for heightened sensitivity, to further secure Murdoch Vision Care from risk of a security incident.

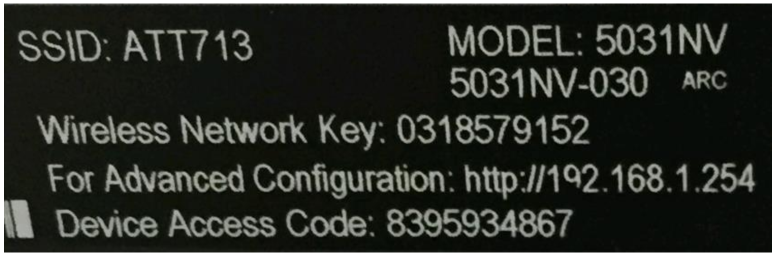
Please don't hesitate to contact Kypher with any questions relating to this Memorandum or if Kypher can be of assistance in any manner.

Dated: August 11th, 2016

Murdoch Vision Care
Logical Network Layout
7/15/16



Murdoch Vision Care
Physical Network Devices
7/15/16



SSID: ATT713 MODEL: 5031NV
5031NV-030 ARC
Wireless Network Key: 0318579152
For Advanced Configuration: http://192.168.1.254
Device Access Code: 8395934867

AT&T Modem with SSID info and passwords printed on device

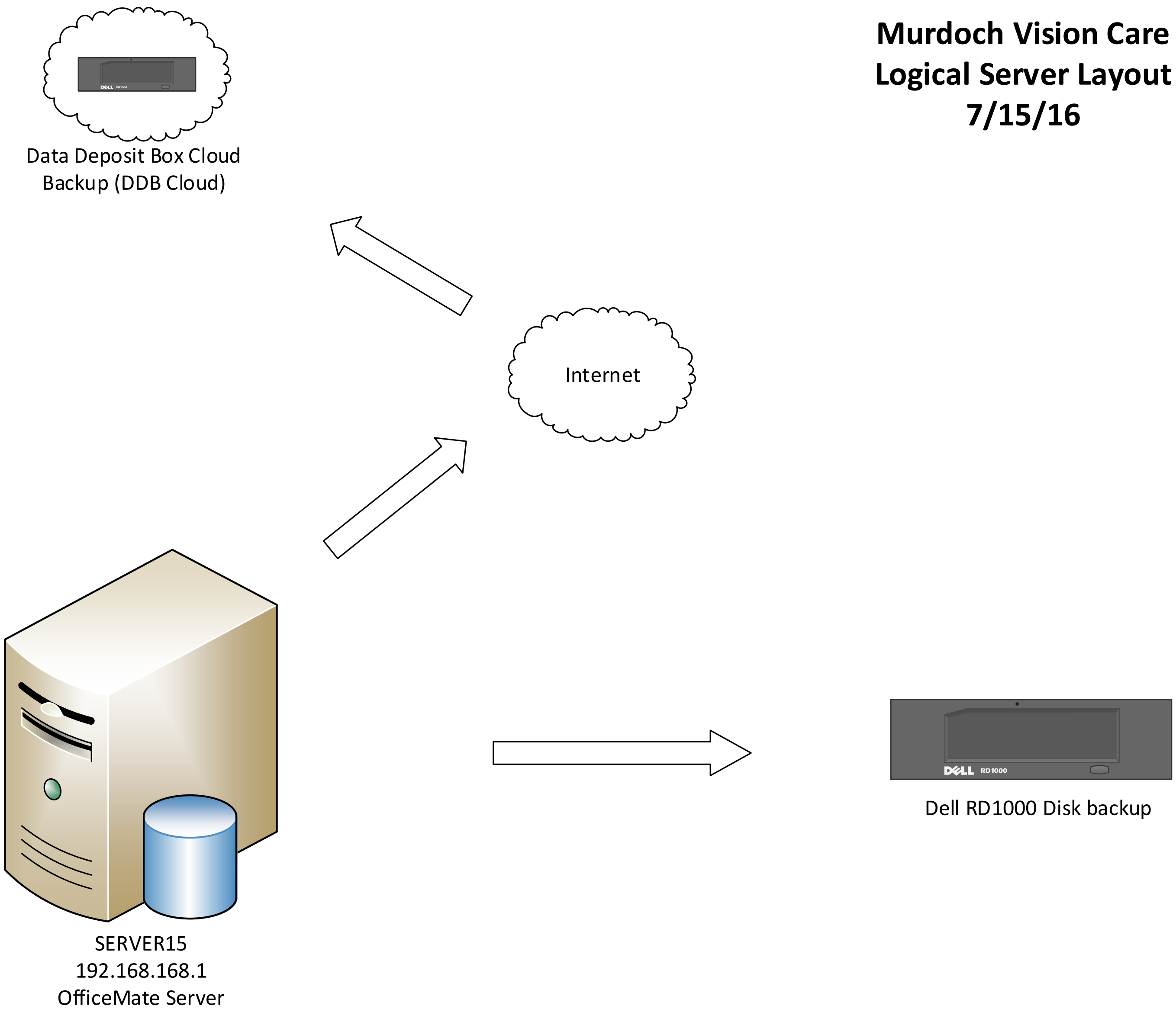
Dynex Network Switch

AT&T Firewall / Modem / Wireless AP
DSL Line & UPS

Linksys Network Switch

TPLink Network Switch

Murdoch Vision Care
Logical Server Layout
7/15/16



Data Deposit Box Cloud
Backup (DDB Cloud)

Internet

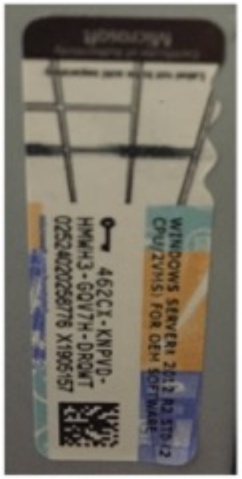
SERVER15
192.168.168.1
OfficeMate Server

Dell RD1000 Disk backup

Murdoch Vision Care
Physical Sever Devices
7/15/16

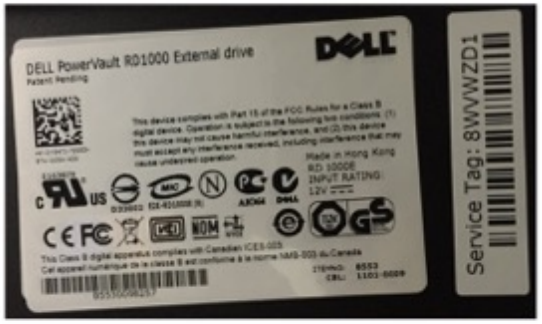
SERVER15 (Front)

SERVER15 (Rear)



SERVER15 (Windows 2012 license)

Dell RD1000 Drive cartridge backup unit (Front)



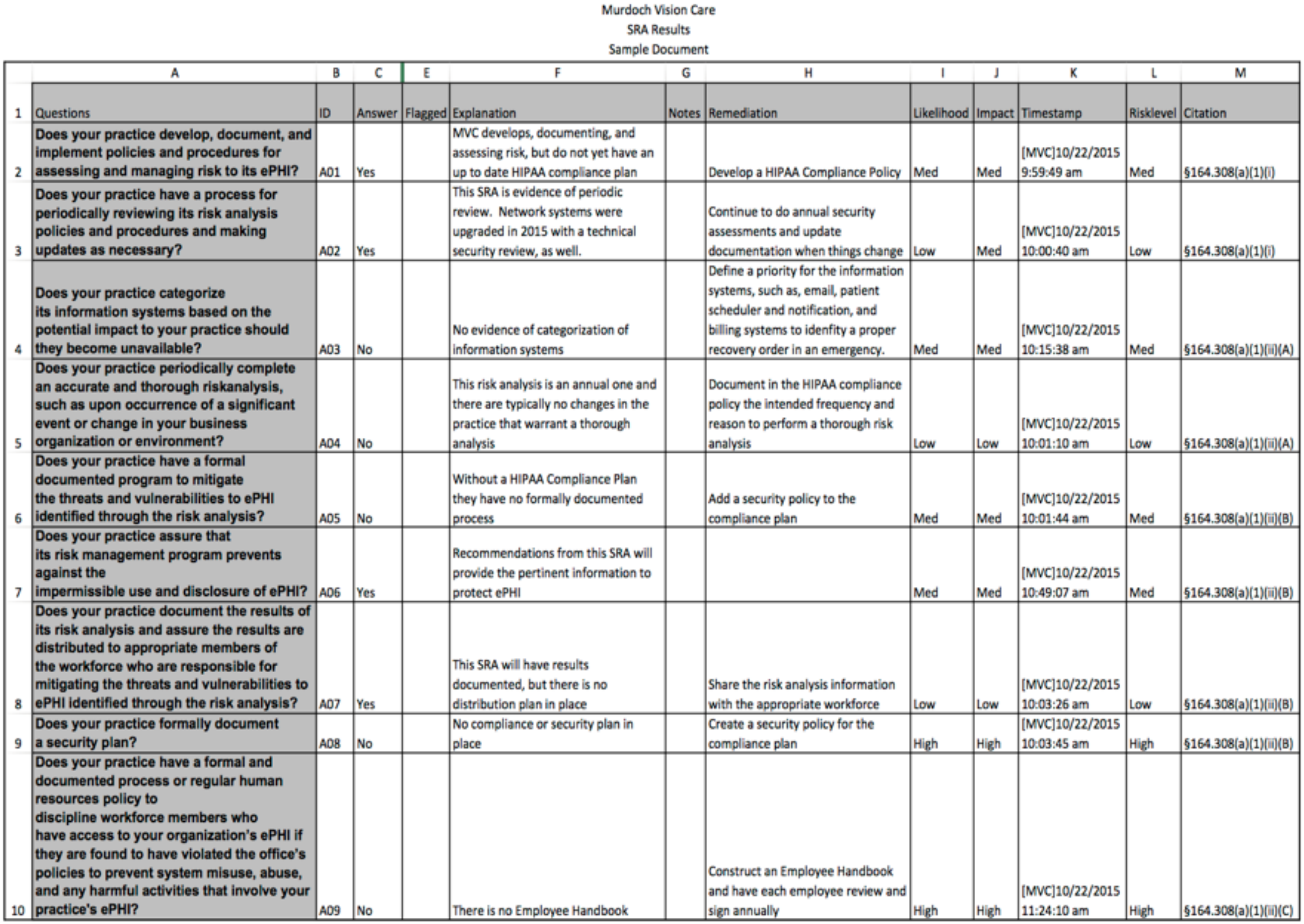
Dell RD1000 Drive cartridge backup unit (Rear)

Murdoch Vision Technical Asset List

Name	Type	Model, Number	Serial Number	RAM installed(Max)	CPU	OS	Internal Disk(s)	Network
SERVER15	Computer/server	Computer Pro Unltd. white box	15078	8GB(32GB Max)	Intel(R) Xeon(R) CPU E3-1231 v3 @ 3.40GHz (architecture: x64; 3401 MHz)	Windows Server2012 Standard	Size 929GB, 882GB Free Space. CD/DVD RW	Intel(R) I210 Gigabit Network Adapter IP-address: 192.168.168.1 Adapter MAC-address: 0C:C4:7A:4C:CA:64
FRONT_LEFT	Computer/workstation	Computer Pro Unltd. white box	13001	8GB(32GB Max)	Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz	Windows 7 Pro SP1	Size 465.8GB, 400GB Free Space CD/DVD RW	Network adapter: Realtek PCIe GBE Adapter IP-address: 192.168.168.39 Adapter MAC-address: 94:DE:80:C3:7D:42
FRONTCENTER	Computer/workstation	Computer Pro Unltd. white box	13135	8GB(32GB Max)	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	Windows 7 Pro SP1	Size 465.8GB, 401GB Free Space CD/DVD RW	Network adapter: Realtek PCIe GBE Adapter IP-address: 192.168.168.38 Adapter MAC-address: 94:DE:80:06:F4:87
FRONT_RIGHT	Computer/workstation	Computer Pro Unltd. white box	13002	8GB(32GB Max)	Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz	Windows 7 Pro SP1	Size 465.8GB, 390GB Free Space CD/DVD RW	Network adapter: Realtek PCIe GBE Adapter IP-address: 192.168.168.42 Adapter MAC-address: 90:2B:34:A4:EC:9D
EXAMROOM-PC	Computer/workstation	Computer Pro Unltd. white box	13017	8GB(32GB Max)	Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz	Windows 7 Pro SP1	Size 465.8GB, 185.7GB Free Space CD/DVD RW	Network adapter: Realtek PCIe GBE Adapter IP-address: 192.168.168.40 Adapter MAC-address: 94:DE:80:01:14:E4
THINKPAD	Computer/workstation	Lenovo	MP050X15	4GB(16GB Max)	AMD A8-5550M x64; 2100 MHz APU with Radeon(tm) HD Graphics	Windows 7 Pro SP1	Size 446.2GB, 395.2GB Free Space CD/DVD RW	Network adapter: Realtek PCIe GBE Adapter IP-address: 192.168.168.30 Adapter MAC-address: 20:1A:06:C5:4E:40
RANDALLOFFICE	Computer/workstation	Dell Optiplex 780	9KKJNM1	4GB(8GB Max)	Intel(R) Core(TM)2 Duo CPU E8500 @ 3.16GHz	Windows 7 Pro SP1	Size 294.3GB, 222.4GB Free Space CD/DVD RW	Network adapter: Intel(R) 82567LM-3 GBE Adapter IP-address: 192.168.168.32 Adapter MAC-address: B8:AC:6F:B1:D6:4A
External Drive	external (removable cartridge) drive	Dell RD1000E	85530098757				160GB - cartridge currently in use Cartridges up to 2TB available	USB connection only (currently attached to SERVER15)
HP LaserJet P1006	Printer	HP P1006 (CB411A)	VND4816314					USB connected to FONT_LEFT
Canon D400-450	MultiFunction Printer	F156600	DTS48613					USB connected to FONT_RIGHT
HP LaserJet 1022	Printer	Q5912A	CNBC6212QR					USB connected to RANDALLOFFICE
GE Digital Messaging System	Answering machine	29869GE2						Analog phone line
Uverse Internet Router	Uverse Internet Router/firewall/Wifi	2Wire/Pace 5031NV	14131A017713					2 analog wire AT&T feed IN Wifi Out 4 ethernet Cat 5 Out. MAC Address 74:90:DC:BC:E0:FC
TP-Link Switch	unmanaged 5 port switch 10/100 by Uverse Router	TL-SF1005D						5 port ethernet Cat5

Murdoch Vision Technical Asset List

Name	Type	Model, Number	Serial Number	RAM installed(Max)	CPU	OS	Internal Disk(s)	Network
Linksys Switch	unmanaged 5 port switch 10/100 one port(2) not functional and when used will disable all remaining 4 ports Under front desk	EZX5552	R9160K441884					5 port ethernet Cat5
Dynex Switch	unmanaged 5 port switch 10/100 in eye imaging room	DX-ESW5	8F05B02028					5 port ethernet Cat5
APC	UPS/Surge protector under front desk, left center	BE350G 350VA	3B1103X32327					
APC	UPS/Surge protector File room near Uverse Router	BE350G 350VA	4B1528P34640					
APC	UPS/Surge protector by server	BE650G 650VA	3B0741X25264					
APC	UPS/Surge protector Randy's office	BE350G 350VA	3B1127X33673					
Retinal Imaging Station Station	Nidex AFC-210 Non-Mydriatic Auto Fundus camera/imaging station	AFC-210	120748					



Murdoch Vision Care
SRA Results
Sample Document

	A	B	C	E	F	G	H	I	J	K	L	M
1	Questions	ID	Answer	Flagged	Explanation	Notes	Remediation	Likelihood	Impact	Timestamp	Risklevel	Citation
2	**Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?**	A01	Yes		MVC develops, documenting, and assessing risk, but do not yet have an up to date HIPAA compliance plan		Develop a HIPAA Compliance Policy	Med	Med	[MVC]10/22/2015 9:59:49 am	Med	§164.308(a)(1)(i)
3	**Does your practice have a process for periodically reviewing its risk analysis policies and procedures and making updates as necessary?**	A02	Yes		This SRA is evidence of periodic review. Network systems were upgraded in 2015 with a technical security review, as well.		Continue to do annual security assessments and update documentation when things change	Low	Med	[MVC]10/22/2015 10:00:40 am	Low	§164.308(a)(1)(i)
4	**Does your practice categorize its information systems based on the potential impact to your practice should they become unavailable?**	A03	No		No evidence of categorization of information systems		Define a priority for the information systems, such as, email, patient scheduler and notification, and billing systems to idenfity a proper recovery order in an emergency.	Med	Med	[MVC]10/22/2015 10:15:38 am	Med	§164.308(a)(1)(ii)(A)
5	**Does your practice periodically complete an accurate and thorough riskanalysis, such as upon occurrence of a significant event or change in your business organization or environment?**	A04	No		This risk analysis is an annual one and there are typically no changes in the practice that warrant a thorough analysis		Document in the HIPAA compliance policy the intended frequency and reason to perform a thorough risk analysis	Low	Low	[MVC]10/22/2015 10:01:10 am	Low	§164.308(a)(1)(ii)(A)
6	**Does your practice have a formal documented program to mitigate the threats and vulnerabilities to ePHI identified through the risk analysis?**	A05	No		Without a HIPAA Compliance Plan they have no formally documented process		Add a security policy to the compliance plan	Med	Med	[MVC]10/22/2015 10:01:44 am	Med	§164.308(a)(1)(ii)(B)
7	**Does your practice assure that its risk management program prevents against the impermissible use and disclosure of ePHI?**	A06	Yes		Recommendations from this SRA will provide the pertinent information to protect ePHI			Med	Med	[MVC]10/22/2015 10:49:07 am	Med	§164.308(a)(1)(ii)(B)
8	**Does your practice document the results of its risk analysis and assure the results are distributed to appropriate members of the workforce who are responsible for mitigating the threats and vulnerabilities to ePHI identified through the risk analysis?**	A07	Yes		This SRA will have results documented, but there is no distribution plan in place		Share the risk analysis information with the appropriate workforce	Low	Low	[MVC]10/22/2015 10:03:26 am	Low	§164.308(a)(1)(ii)(B)
9	**Does your practice formally document a security plan?**	A08	No		No compliance or security plan in place		Create a security policy for the compliance plan	High	High	[MVC]10/22/2015 10:03:45 am	High	§164.308(a)(1)(ii)(B)
10	**Does your practice have a formal and documented process or regular human resources policy to discipline workforce members who have access to your organization's ePHI if they are found to have violated the office's policies to prevent system misuse, abuse, and any harmful activities that involve your practice's ePHI?**	A09	No		There is no Employee Handbook		Construct an Employee Handbook and have each employee review and sign annually	High	High	[MVC]10/22/2015 11:24:10 am	High	§164.308(a)(1)(ii)(C)