Final IA Plan

Risk Management

Ari Mendez, Stephan Battle, Daniel Weinert, and Jeremy Kadis,

IA Defenders G 1 1

CSS2752-001

Metropolitan State University of Denver

Professor Williams

8th December 2020

Intentionally Blank Page

G1 Cyber Defender Pros

Contents

Executive Summary

Information assurance can often be an afterthought for many organizations. However, through enlisting the guidance of G1 Cyber Defender Pros, the health insurance organization, Metro Medical Center (MMC) can rest assured that our thorough assessment of risk, and the subsequent creation of a documented risk management treatment plan shall insure the protection of the organization from future security related incidents, identify current concerns and provide a detailed and informed decision on how to move forward from these incidents, as well as prevent them before they are even given the chance to conspire through the implantation of the various recommendations that will be set forth in this risk management plan. The risk management plan begins with the creation of the classification of assets, from there a risk assessment on MMC's various assets is preformed, followed by the creation of a risk management plan and the incident handler/response, finally, our final recommendations for information assurance shall be given. Having a readily available risk information plan provides MMC with a competitive edge in that taking the steps necessary to assure company information and assets ensures customer satisfaction with performance, providing MMC with the appropriate social approval rating. However, taking the time to assure company information and assets also increases the likelihood that MMC can avoid the high costs associated with data breaches. G1 Cyber Defender Pros commits to fulfilling the mission statement set forth by MMC: providing right on time healthcare to clients while enabling customers as well as MMC's vision of providing ubiquitous and secure mobile access to patients through patient portals to enable preventive medicine through transparency. In order to fulfil the mission and vision of MMC, the information assurance treatment plan relies heavily on the concepts presented by the pillars of cybersecurity, also known as the CIA (Confidentiality, Integrity, Availability) triad. Through implementing solutions to problems which threaten the confidentiality, integrity, and availability of MMC's assets, we are concurrently upholding the standards of cybersecurity excellence as well as fulfilling the mission and vision of the organization.

G1 Cyber Defender Pro Team Members

NAME	Title	Company	E-Mail	Phone
Ari Mendez	Director, Security, Risk & Compliance	G1 Cyber	Amendez@g1.com	Office: 303-303-30330
Jeremy Kadis	Senior Risk Analyst	G1 Cyber	Jkadis@g1.com	Office: 721-721-72111
Daniel Weinert	Senior Risk Analyst	G1 Cyber	Dweinert@g1.com	Office:720-720-72000
Stephan Battle	Senior Risk Analyst	G1 Cyber	SBattle@g1.com	Office: 310-310-31010

Classification of Assets

The goal of our information assurance organization is to implement an information assurance plan in order to help secure the confidentiality, integrity, and availability of our hospital client's assets. At the dawn of an increasingly digitalized age in the health care industry, it is vital for the assurance of information and the proper implementation of security controls to be put in place in order to protect both customer and organization information (Schou & Hernandez, 2015) In addition to the implementation of a well crafted IA plan, the organization, operating as a hospital within the American health care system must adhere to extensive security protocol, in order to abide by US laws and regulations pertaining to the confidentiality of patient medical records. HIPPA laws and regulations as put forth by the American federal government reserve the right to confidentiality of a patient's medical record (Benefield, Ashkanazi,, & Rozensky, 2006). In compliance with HIPPA laws, this information assurance plan shall not only help to prevent loss of assets and security risks posed to the organization, but also meet federal guidelines for the handling of patient health information. The pillars of cybersecurity, and as an extension of which, information assurance are represented in the CIA triad and shall serve as the basis for our classification of assets, and the foundation of our IA plan. Confidentiality refers to the idea that an asset must be kept within its privacy classification, Integrity refers to the idea that an asset must be safe from unauthorized alteration or destruction, while availability refers to the idea that an asset must be readily available when needed (Kremling & Sharp Parker, 2018).

Critical Rating Recommendation:

Name	Confidentiality	Availability	Integrity
Admin Office			
EHR	severe	severe	severe
Appointment & Scheduleing application	moderate	moderate	low
CRM/Billing	severe	severe	severe
Strategic MIS	moderate	moderate	severe
Inpatient/Outpatient	severe	severe	severe
Facilities Office			
Security control	severe	severe	severe
CRM/Inventory and stock	Moderate	moderate	severe
Pharmacy Office			
EHR/Pharmacy	Severe	severe	severe
EHR/Insurance	Severe	Severe	Severe
Drug interaction DB	Severe	Severe	Severe
CRM/Billing	Severe	Severe	Severe
Computerized physician order entry	severe	moderate	severe
Rx30 Pharmacy Softw are	severe	severe	severe
PDX Pharmacy System	severe	severe	severe
Dental Department			
CAD/CAM & intraoral imaging	moderate	moderate	moderate
Digital radiography	moderate	moderate	moderate
Patient Appointment	severe	severe	severe
Patient evaluation and treatment planning	severe	severe	severe
Occlusion and TMJ analysis & diagnosis	severe	severe	severe
Compliance designing using CAD	moderate	moderate	moderate
Cone-beam computed tomography	severe	severe	severe
HR Department			
Mettl	low	low	moderate
Outbound Hiring Solutions	moderate	low	moderate
Rescue Time	severe	severe	severe
Trello	low	low	moderate
HRIS/payroll management	severe	severe	severe
Background Check	severe	severe	severe
Business Office			
Registration Application	moderate	low	moderate
Customer Service, Collections & Insurance Verification	Severe	moderate	severe
CRM/ACCOUTING	severe	severe	severe
Patient DB	severe	severe	severe
Audiology Department			
Audiology imaging softw are	severe	moderate	moderate
TIMS Audiology Softw are	moderate	moderate	severe
EHR/Audiology APP	severe	severe	severe
iPad Automator	low	low	moderate
Radiology Department			
ProtonPACS	severe	moderate	severe
EHR/Radiology	severe	severe	severe
Pediatrics Department			
EHR	severe	severe	severe
PEDIS TAT SETUP	low	low	moderate
Care	severe	severe	severe
Lab Department			
Psyche Systems	severe	moderate	severe
EHR/LAB	severe	severe	severe
Avalon Laboratory System	severe	moderate	severe
Mental Health Department			
Telehealth	severe	moderate	moderate
SAMHSA	Severe	severe	severe
Substance abuse Database	severe	severe	severe
Suicide risk management Database	severe	severe	severe
EHR/Mental Health	severe	severe	severe
Food Services			
Dietary Manager	low	low	moderate
Information Technology Department			
Cisco ISE	severe	severe	severe
Crowdstrike	severe	severe	severe
FireMon	severe	severe	severe
McAfee	severe	severe	severe
Oracle Enterprise Manager (OEM)"	severe	severe	severe
Palo Alto	severe	severe	severe
SCCM	severe	severe	severe
SolarWinds	severe	severe	severe
Splunk Core & ES	severe	severe	severe
Spotlight	severe	severe	severe
Tanium	severe	severe	severe
Tenable	severe	severe	severe
VMWare LogInsight	severe	severe	severe
VMWare VROPs	severe	severe	severe
vRealize Network Insight	severe	severe	severe

Classification of Assets

Assests	Classification	Department	Critical Rating	Assignee
EHR	Restricted	Admin Office	Severe	Hospital Administrator
Appointment & Scheduleing application	Restricted	Admin Office	Moderate	Hospital Administrator
CRM/Billing	Confidential	Admin Office	Severe	Hospital Administrator
Strategic MIS	Restricted	Admin Office	Moderate	Hospital Administrator
Inpatient/Outpatient	Confidential	Admin Office	Severe	Hospital Administrator
Security control	Confidential	Facilities Office	Severe	Director of Facilities
CRM/Inventory and stock	Restricted	Facilities Office	Moderate	Director of Facilities
EHR/Pharmacy	Restricted	Pharmacy Office	Severe	Director of Pharmacy
EHR/Insurance	Confidential	Pharmacy Office	Severe	Director of Pharmacy
Drug interaction DB	Confidential	Pharmacy Office	Severe	Director of Pharmacy
CRM/Billing	Confidential	Pharmacy Office	Severe	Director of Pharmacy
Computerized physician order entry	Restricted	Pharmacy Office	Severe	Director of Pharmacy
Rx30 Pharmacy Software	Confidential	Pharmacy Office	Severe	Director of Pharmacy
PDX Pharmacy System	Confidential	Pharmacy Office	Severe	Director of Pharmacy
CAD/CAM & intraoral imaging	Restricted	Dental Department	Moderate	Chief of Dental
Digital radiography	Restricted	Dental Department	Moderate	Chief of Dental
Patient Appointment	Confidential	Dental Department	Severe	Chief of Dental
Patient evaluation and treatment planning	Confidential	Dental Department	Severe	Chief of Dental
Occlusion and TMJ analysis & diagnosis	Confidential	Dental Department	Severe	Chief of Dental
Compliance designing using CAD	Restricted	Dental Department	Moderate	Chief of Dental
Cone-beam computed tomography	Confidential	Dental Department	Severe	Chief of Dental
Meitl	Restricted	HR Department	Low	Director of HR
Outbound Hiring Solutions	Restricted	HR Department	Moderate	Director of HR
Rescue Time	Restricted	HR Department	Severe	Director of HR
Trello	Restricted	HR Department	Low	Director of HR
HRIS/payroll management	Confidential	HR Department	Severe	Director of HR
Background Check	Confidential	HR Department	Severe	Director of HR
Registration Application	Confidential	Business Office	Moderate	Director of Business
Customer Service, Collections & Insurance Verification	Confidential	Business Office	Severe	Director of Business
CRM/ACCOUTING	Confidential	Business Office	Severe	Director of Business
Patient DB	Confidential	Business Office	Severe	Director of Business
Audiology imaging software	Restricted	Audiology Department	Moderate	Chief of Audiology
TIMS Audiology Software	Restricted	Audiology Department	Moderate	Chief of Audiology
EHR/Audiology APP	Restricted	Audiology Department	Severe	Chief of Audiology
iPad Automator	Restricted	Audiology Department	Low	Chief of Audiology
ProtonPACS	Restricted	Radiology Department	Severe	Chief of Radiology
EHR/Radiology	Confidential	Radiology Department	Severe	Chief of Radiology
EHR	Confidential	Pediatrics Department	Severe	Chief of Pediatrics
PEDISTAT SET UP	Restricted	Pediatrics Department	Low	Chief of Pediatrics
Care	Confidential	Pediatrics Department	Severe	Chief of Pediatrics
Psyche Systems	Restricted	Lab Department	Severe	Chief of Nursing
EHR/LAB	Confidential	Lab Department	Severe	Chief of Nursing
Avalon Laboratory System	Restricted	Lab Department	Severe	Chief of Nursing
Telehealth	Confidential	Mental Health Department	Moderate	Medical Director
SAMHSA	Confidential	Mental Health Department	Severe	Medical Director
Substance abuse Database	Confidential	Mental Health Department	Severe	Medical Director
Suicide risk management Database	Confidential	Mental Health Department	Severe	Medical Director
EHR/Mental Health	Confidential	Mental Health Department	Severe	Medical Director
Dietary Manager	Restricted	Food Services	Low	Chief of Staff
Cisco ISE	Confidential	IT Department	Severe	Director of IT
Crowdstrike	Confidential	IT Department	Severe	Director of IT
FireMon	Restricted	IT Department	Severe	Director of IT
McAfee	Confidential	IT Department	Severe	Director of IT
Oracle Enterprise Manager (OEM)"	Restricted	IT Department	Severe	Director of IT
Palo Alto	Confidential	IT Department	Severe	Director of IT
SCCM	Restricted	IT Department	Severe	Director of IT
SolarWinds	Restricted	IT Department	Severe	Director of IT
Splunk Core & ES	Restricted	IT Department	Severe	Director of IT
Spotlight	Restricted	IT Department	Severe	Director of IT
Tanium	Confidential	IT Department	Severe	Director of IT
Tenable	Confidential	IT Department	Severe	Director of IT
VMWare LogInsight	Restricted	IT Department	Severe	Director of IT
VMWare VROPs	Restricted	IT Department	Severe	Director of IT
vRealize Network Insight	Confidential	IT Department	Severe	Director of IT

Recommendations

The first stage of implementation of the IA plan shall deal in asset categorization. In order to categorize the assets as outlined as belonging to the organization through the information supplied to us by the organization, we have first started our process by organizing the assets by department, we then assigned responsibility of those assets to the head and or directors of each governing department (ie. An asset belonging to the pharmacy office shall be assigned to the director of pharmacy). We then classified each asset based on its availability level (either completely confidential, or merely restricted). From there, we were able to determine and assign a critical rating to each asset based upon our analysis of the CIA triad (Qian, Tipper, Krishnamurthy, & Joshi, 2010). In using the principles of confidentiality, integrity, and availability we are able to assign a sort of high-level analysis on what risk level the asset might be in. For example, we have classified each asset as either having a low, moderate, or severe critical rating. In order to make better sense of these ratings and the terms in which we have defined them, the following visual is used in order to assess the critical rating of each asset.

Confidentiality	Integrity	Availability
Low: The unauthorized release of information is expected to have a low- level negative impact on the organization/asset/customer.	**Low:** The unauthorized destruction of or alternation of information is expected to have a low-level negative impact on organization/asset/customer.	**Low:** The lack of access to the information is expected to have a low-level negative impact on the organization/asset/customer.
Moderate: The unauthorized release of information is expected to have a mid-level negative impact on the organization/asset/customer.	**Moderate:** The unauthorized destruction of or alternation of information is expected to have a mid-level negative impact on organization/asset/customer	**Moderate:** The lack of access to the information is expected to have a mid-level negative impact on the organization/asset/customer.
Severe: The unauthorized release of information is	**Severe:** The unauthorized destruction of or alternation	**Severe:** The lack of access to the information is expected to

expected to have a high-level negative impact on the organization/asset/customer.	of information is expected to have a high-level negative impact on organization/asset/customer	have a high-level negative impact on the organization/asset/customer.

From these recommendations, the final critical rating as seen on the asset classification considers all three concepts of confidentiality, integrity, and access in order to come forth with a final critical rating recommendation for asset classification purposes.

Risk Assessment

The purpose of this risk assessment is to evaluate the adequacy and inadequacies of the security bestowed upon Metro Medical Center's various assets. This risk assessment shall provide a structured qualitative assessment of the current operational environment in order to evaluate the effectiveness of the environment as well as to identify and create a plan of action in order to address inadequacies or security weaknesses within the existing environment. This report shall address sensitivity, threats, vulnerabilities, risks and safeguards for each asset, with specific attention to assets deemed to be at most critical risk. The assessment shall them provide recommendations for cost-effective safeguards to mitigate threats, in order to address existing security issues, as well as potential issues. The scope of this risk assessment shall access Metro Medical Center's use of resources and controls to eliminate and/or create an action plan to manage vulnerabilities exploitable by threats internal and external to Metro Medical Center. Should the integrity of Metro Medical Center's assets me threatened, the following adverse effects may occur:

- Issues pertaining to confidentiality: unauthorized disclosure of data
- Issues pertaining to integrity: unauthorized modification to the application, its data, or both
- Issues pertaining to availability: denial of service, access to data, or both to authorized users

This Risk Assessment Report shall utilize the pillars of cybersecurity, also known as the CIA triad in order to evaluate the Confidentiality (protection from unauthorized disclosure of application and data information), Integrity (protection from improper modification of information), and Availability (loss of application access) of Metro Medical Center's assets. The recommendations set forth by G1 Cyber shall provide the framework for Metro Medical Center's leadership to take action to prevent security related incidents, through the creation of a Plan of Action and Milestone (POAM).

The following tables will identify the owner for each asset for the purpose of giving a point of contact in case there is potential impact should there be a loss of data confidentiality, integrity and/or availability (CIA). Key officials for management, guidance, and authorization are also listed in the following tables.

The following tables will identify the owner for each asset for the purpose of giving a point of contact in case there is potential impact should there be a loss of data confidentiality, integrity and/or availability (CIA). Key officials for management, guidance, and authorization are also listed in the following tables.

Admin Office Asset Owners

	Department Leader	Technical Steward	DAA

	Department Leader	Technical Steward	DAA
Name	Tristan Lestrange	Patricia Spitznagel	Benvolio Mein
Title	Hospital Administrator	Business Analyst	Application Manager
Address	3418 Wetrod Drive, CO	4114 Robinson Court, CO	5003 Caynor Circle, CO
Phone	720-548-6578	720-658-5574	720-587-9369
E-mail	tlestrange@mmc.org	psptiznagel@mmc.org	bmein@mmc.org

Admin Office Critical Assets

Applications	Description	Environment	Users
EHR	Digital version of a patient's paper chart	Runs on the cloud with access from local computer	Medical Staff
Appointment & Scheduling application	Using Microsoft 365 outlook calendar to schedule appointments	Office 365	Front Desk, Assistants
CRM/Billing	Using salesforce as CRM system	Salesforce Cloud	HR, Accounting

Facilities Critical Asset Owners

Name	Waneta Read	Lenard Batchelor	Genna Desimone
Title	Dir. of Facilities	CRM Engineer	Facilities Manager
Address	1530 McKinley Avenue, CO	3021 River Road, CO	1456 Aspen Court, CO
Phone	720-578-9824	720-558-4678	720-228-6577
E-mail	wread@mmc.org	lbatchelor@mmc.org	gdesimone@mmc.org

Facilities Critical Asset

Applications	Environment	Users
CRM	Salesforce Cloud	Accounting, Facilities Managers
I&S	Hosted on internal hospital server	Facilities Staff

Pharmacy Office Assets Owners

	Department Leader	Technical Steward	DAA
Name	Jesse Huber	Ismael Mcdaniel	Denese Winstead

Title	Dir. of Pharmacy	Clinical Application Engineer	Pharmacy Manager
Address	3007 Hope Street, CO	403 Simons Hollow Road, CO	3208 Orphan Road, CO
Phone	720-579-6657	720-466-5484	720-586-5575
E-mail	jhuber@mmc.org	imcdaniel@mmc.org	dwinstead@mmc.org

Pharmacy Office Critical Asset

Applications	**Description**	**Environment**	**Users**
CRM	Using salesforce as CRM system	Salesforce Cloud	Accounting, Pharmacy Manager
Drug DB	FDA Drug Database	Hosted on Cloud server	Pharmacy Staff
Rx30/PDX Pharmacy Software	Pharmacy management system	Run on hospital servers	Pharmacy Staff

Dental Department Assets Owners

	Department Leader	**Technical Steward**	**DAA**
Name	Gaylene Zamora	Wallace Byrne	Donnell Soliz
Title	Chief of Dental	Clinical Applications Analyst	Dental IT Manager
Address	3126 Horner Street	4032 Rosewood Court	4397 Nickel Road

Dental Department Critical Asset

Applications	**Description**	**Environment**	**Users**
CAD/CAM	Technology constructs restorations, like crowns, veneers, inlays, on lays and bridges, from a single block of ceramics, which makes the final product more precise compared to traditional fabrication methods.	Run on internal Hospital Server	Hospital staff relating to dental
Cone-beam	special type of x-ray equipment	Runs on x-ray equipment	Dental Nurses/Assistant
Phone	720-548-6698	720-887-4687	720-548-6697
E-mail	@mmc.org	@mmc.org	@mmc.org

HR Department Assets Owners

	Department Leader	**Technical Steward**	**DAA**
Name	Liviu Warfield	Lauran Gilliland	Brander Schubert
Title	Dir. of HR	Business Analyst	HR Manager

Address	3121 Colony Street	4152 Chandler Drive	2240 Walnut Avenue
Phone	720-574-9965	720-778-6571	720-411-5477
E-mail	lwarfield@mmc.org	lgilliland@mmc.org	bschubert@mmc.org

HR Department Critical Asset

Applications	**Description**	**Environment**	**Users**
Mettl	Online recruitment process tool	SaaS	HR staff
Trello	Trello's boards, lists, and cards enable teams to organize and prioritize projects in a fun, flexible, and rewarding way.	SaaS	Entire HR department
HRIS/payroll management	Salesforce	Salesforce Cloud	Accounting, HR Managers

Business Office Assets Owners

	Department Leader	**Technical Steward**	**DAA**
Name	Shonda Lovett	Quincy Cash	Halward Causey
Title	Dir. of Business	Business Analyst	Business Office Manager
Address	1763 Coolidge Street, CO	1385 Charles Street, CO	711 Davis Place, CO
Phone	720-557-6598	720-578-6657	720-861-6571
E-mail	slovett@mmc.org	qcash@mmc.org	hcausey@mmc.org

Business Office Asset

Applications	**Description**	**Environment**	**Users**
Customer Service	Salesforce	Salesforce Cloud	Customer Service representetives
Patient DB	HanDBase	Internal hospital server	General Hospital Staff

Audiology Department Assets Owners

	Department Leader	**Technical Steward**	**DAA**
Name	Romano Kong	Riddley Ellison	Cassidee Jude
Title	Chief of Audiology	Clinical Application Analyst	Audiology Manager
Address	4503 Ridenour Street, CO	1465 Timbercrest Road, CO	4496 Dog Hill Lane, CO
Phone	720-548-9871	720-811-6544	720-732-5698
E-mail	rkong@mmc.org	rellison@mmc.org	cjude@mmc.org

Audiology Department Critical Asset

Applications	Description	Environment	Users
TIMS Audiology Software	Hearing test software	On audiology computers	Audiology staff and doctors
iPad Automator	Workflows consisting of a sequence of discrete modules called actions.	Audiology iPad	Audiology staff

Radiology Department Assets Owners

	Department Leader	Technical Steward	DAA
Name	Navon Foreman	Ketil Jacob	Jenyfer Worthington
Title	Chief of Radiology	Clinical Application Analyst	Radiology Manager
Address	304 Pursglove Court, CO	3675 Pride Avenue, CO	2998 New York Avenue, CO
Phone	720-548-5465	720-479-3467	720-488-5576
E-mail	nforeman@mmc.org	kjacob@mmc.org	jworthington@mmc.org

Radiology Department Critical Asset

Applications	Description	Environment	Users
ProtonPACS	Picture archiving and communication system for any imaging environment	On site hosting	Radiology staff, Medical staff

Pediatrics Department Assets Owners

	Department Leader	Technical Steward	DAA
Name	Sancia Baer	Griffith Crawford	Lion Bruner
Title	Chief of Pediatrics	Clinical Application Analyst	Pediatrics Manager
Address	3313 Watson Street, CO	3696 Bolman Court, CO	2163 Harley Brook Lane, CO
Phone	720-634-1468	720-548-6698	720-788-6557
E-mail	sbaer@mmc.org	grawford@mmc.org	lbruner@mmc.org

Pediatrics Department Critical Asset

Applications	Description	Environment	Users

PEDISTAT SET UP	Rapid reference for RNs, paramedics, physicians and other healthcare professionals caring for pediatric patients in the emergency or critical care environment.	On device	Pediatrics Department

Lab Department Assets Owners

	Department Leader	**Technical Steward**	**DAA**
Name	Parks Hardison	Lionnel Spangler	Madock Mundy
Title	Medical Lab Director	Lab Engineer	Lab Manager
Address	1432 Huntz Lane	2844 Berkshire Circle	2081 Oakridge Lane
Phone	720-549-5587	720-144-5678	720-411-5587
E-mail	phardison@mmc.org	lspangler@mmc.org	mmundy@mmc.org

Lab Department Critical Asset

Applications	**Description**	**Environment**	**Users**
Psyche Systems	highly-configurable laboratory information systems	On Site hosting	Lab Managers
Avalon Laboratory System	Highly sophisticated group of programs designed to manage all production and billing needs of laboratories.	SaaS	Lab Department

Mental Health Department Assets Owners

	Department Leader	**Technical Steward**	**DAA**
Name	Emlynn Hartley	Katiana Maxey	Pernell Swanson
Title	Chief of Mental Health	Clinical Application Analyst	Mental Health Department Supervisor
Address	1942 Agriculture Lane, CO	1196 Roosevelt Road, CO	3939 Meadow Drive, CO
Phone	720-558-6974	720-788-4635	720-789-4164
E-mail	ehartley@mmc.org	kmaxey@mmc.org	pswanson@mmc.org

Mental Health Department Critical Asset

Applications	**Description**	**Environment**	**Users**

Telehealth	Online meeting healthcare system that allows patients at home to connect with staff	SaaS	Medical Staff, patients
SAMHSA	Agency within the U.S. Department of Health and Human Services that leads public health efforts to advance the behavioral health of the nation.	On government server	MA staff
Substance Abuse/Suicide Risk DB	Main HER system	On site hosting	Medical Staff

Information Technology Assets Owners

	Department Leader	**Technical Steward**	**DAA**
Name	Collby Fraley	Udolph Schwarz	Kimbel Burrows
Title	Dir. of IT	Technical Engineer	IT Manager
Address	2112 Lynn Ogden Lane, CO	109 Park Street, CO	2619 Perry Street, CO
Phone	720-487-8845	303-789-4654	720-457-5468
E-mail	@mmc.org	@mmc.org	@mmc.org

Information Technology Critical Asset

Applications	**Description**	**Environment**	**Users**
Cisco ISE	Enables a dynamic and automated approach to policy enforcement that simplifies the delivery of highly secure network access control.	On main system	IT staff
Crowdstrike	Cloud-native endpoint security platform	SaaS	IT staff, IT Security
FireMon	Agile network security policy platform	On site	IT staff, IT Security
McAfee	Anti-Virus application	On each computer	IT Admin
Palo Alto	Firewall system	On network system	IT staff, IT Security
Splunk Core & ES	Security information and event management solution	On network system	IT staff, IT Security
Tanium	Unified Endpoint Management and Security	On site hosting	IT Staff

Tenable	Cyber Exposure company	SaaS	IT Staff
VMware	Virtual Machine App	On site hosting	IT department, other hospital departments

Data Type Categorization

The data category of an asset should be at least rated the highest impact level that has been determined for each type of asset for each security objective of Confidentiality, Integrity, Availability. The following table will show the most critical assets and what data types they store. When you will see a place of reference for the law/guideline and then a basic CIA triad overview to quickly analyze how much risk is involved with each data type.

Data Type Security Characterization

Asset	Data Type	Governing Law/Guidance	Guideline Reference	Confidentiality	Integrity	Availability
EHR	Patient Medical Data, Lab	HIPPA, HITECH Act, MACRA, CO Data Law	DHS	High	High	High
	and test results, Pii					
CRM/Billing	Limited Patient Data, Pii, Financial Data	MACRA, CO Data Law	FPB, FTC	High	High	High
Telehealth	Limited Patient Data	HIPPA	DHS	High	Mid	Mid
Patient DB	Pii, Limited Patient Data	HIPPA, CO Data Law	DHS, CO Gov	High	High	High
Outbound Hiring Solutions/Mettl	Pii	CO Data Law	CO Gov	High	Mid	Low

Critical Risk to Data

This following table will contain the most critical risks we identify through our findings and interviews relating to data.

Critical Risk to Data

Data Type / Law / Guidance	Findings	Risk	Recommend Solution

HIPPA	Print medical documents from home, 30% of employee did not know any HIPPA policy	Violating federal law,	Make sure that every employee receives a yearly HIPPA training and data privacy training
Old employee records, Pii	Old employee accounts, and other accounts have not been closed	Losing track of data, risk to loss of data or it being stolen	Implement a retention schedule that deletes old accounts
Medical Records, Pii	Data sent from remote clinics to main server are not secured properly	Data being lost, stolen or unavailable. Huge risk to HIPPA and CO data law violation	Implement adequate security controls and encryption

Risk Assessment

Risk Assessment Results

Risk Assessment Results for High rating

Asset	Evidence Required	Evidence	Control Effectiveness	Exposure Potential[1]	Likelihood[2]	Impact[3]	Risk Rating
CRM/Billing	**n/a**	**n/a**	**Effective**	**High**	**Likely**	High	Critical
HRSI Payroll Management	**n/a**	**n/a**	**Effective**	Medium	Likely	High	Critical
Customer Service Collections and Insurance Verification	**n/a**	**n/a**	**Effective**	High	Unlikely	High	Critical
Patient Database	**n/a**	**n/a**	**Effective**	High	Unlikely	High	Critical
Substance Abuse Database	**n/a**	**n/a**	**Effective**	High	Likely	High	Critical
CRM/Accounting	**n/a**	**n/a**	**Effective**	Medium	Likely	High	Critical

SECURITY VULNERABILITY SCANS

Vulnerability for Testing	Remediation	Risk Factor
Only one form of authentication is used to access the systems.	Use a system of Multi-Factor authentication such as biometrics or a card system that will implement something	Critical
Passwords are changed only every 6 months and require an 8-character minimum	Require that the password length be extended by and extra four characters and the passwords need to be updated in the system once every 60 days.	Critical
There are several accounts that have been abandoned, several of those accounts were from employees that were fired within the last 6 months	Make sure that the accounts of all employees that were terminated have been deactivated.	Critical
Several Patches of Apache Struts are missing in the system	The system should be updated and managed to make sure that updates are automatically updated and checked for integrity.	Critical
There are no configuration baselines for 8 systems	All systems should have baselines for their critical software. In the company policy jacket, there should be an incorporation of baselines to control manage each system.	Critical
Logs are being overwritten every two years	All logs older than 2 years should be kept in a database where it can be acquired at later times. Also the logging system should delete the program for overwriting data	Critical
Medicaid Database is not adequately secured	Since this not only deals with PII but also patient insurance information, security systems need to put in place to make sure that only authorized personnel may access the information.	Critical
Scope Creep for several Long term employees who had changed roles	With scope creep, there should always be some sort of Access Control in place whether it be MAC, RBAC or DAC. These will eliminate the issues of scope creeping	Critical
Scans showed that several of the critical risks had vulnerabilities	These need to be addresses immediately and with proper assurance to the assets. Risk analysis should be ran every quarter to ensure that vulnerabilities are being mitigated	Critical

HIPPA Server is at the end of its life cycle	Prior to the end of any servers life cycle, the company should have a plan to discuss about the next action to take with the CIO about the servers that hold information regarding patient data and HIPPA records and policies.	Critical
Vulnerability for Interviews	**Remediation**	**Risk Factor**
HIPPA training is not consistent throughout all departments	In the policy Jacket it should be disclosed that HIPPA and other trainings are mandatory for all employees and future employment is contingent on that training being complete.	Critical
Employees often left patient records on their desks	As part of the security protocol, after records have been viewed, if not being actively worked on all patient records and files need to be locked up and kept in a secure place until needed again.	Critical
HIPPA RA was done 5 years ago, but nothing followed or was documented.	All RA need be documented and kept for records as well as the CIO and other security personnel need to follow through with assessment protocols on mitigating vulnerabilities.	Critical
Management was not focusing on the security measures of the organization	A top down approach would best suit the need for higher level management to be actively involved in the security process and allow for employees to see its importance.	Critical
A third of the employees interviewed did not know what HIPPA was.	All employees must go g=through a training seminar at least once a year, refreshing information on the HIPPA rules and regulations that must be followed.	Critical
Employees spoke of a breach that was Bit Reported	Breaches in security are supposed to be disclosed when needed, however there should be policies in place to make sure that speaking of breaches in a certain light should be prohibited.	Critical
Employees did not know who to contact in case of a breach.	In the policy jackets all employees should know who to contact in in what manner of time frame in case of a breach.	Critical
Patients and employees can print medical documents from home	If PII and other medical documents are required to be printed from home, there needs to be a VPN portal to allow access to those documents in a secure fashion.	Critical

Remote hospital is still using SSL to send sensitive data to the main hospital.	All information needs to be sent over a secure protocol such as HTTPS or DNS preferably in order to mitigate risk of breach or exposure	Critical
Remote access point allows for rouge devices to logon	All remote access points should only allow those with authorized credentials to logon to the network.	Critical
Vulnerability for Documentation	**Remediation**	**Risk Factor**
At least half of the assets have no System Security Plan	All departmental assets need to have a security plan in place so that the assets in question can be properly protected	Critical
The assets with SPP are missing pertinent information such as flowcharts and classifications	All departmental assets need to have a risk and asset classification is done at least once every year in order to help with the security protocols. Make sure that all information is properly documented as well.	Critical
1/3 of the assets have no Disaster recovery plan	All assets and documentation must have a Disaster recovery plan and that plan should be evaluated once every quarter to ensure that in case of failure to prevent disaster, the plan still works.	Critical
1/10 of the Employees have outdated computer behavior rules	As part of their on boarding training and continued education, all employees should have to go through proper computer training	Critical
Background checks for several Vendors have not been done	All vendors must have background checks done before being allowed to work with the organization. Policies should include methodology to background checks.	Critical
There were several missing policies for provisioning, deprovisioning, orientation and termination.	All policies for employee introduction and termination for the company should be well documented and all employees should know the provisions for employment and termination.	Critical
Several vendor service agreements have been missing	Before allowing partnership with the organization, all vendors must fill out and sign a service level agreement which should be kept with the department records for keeping.	Critical

The cloud providers have not and do not offer a path for problem escalation.	The organization should make sure to partner with an IaaS that will allow for problem escalation and service requests for all issues.	Critical
There is no documented vendor management plan	As stated in the policy jacket management plans for the vendors must be documented and kept for at least 5 years so that all plans may be kept in order from time of inception.	Critical
There is no MOU, however there is several interconnected systems.	A memorandum of understanding is a document that describes the broad outlines of an agreement that two or more parties have reached. All of those systems should have a place in the MOU to make sure that all of the systems have a well documented summary.	Critical

RISK ASSESMENT RECOMMENDATIONS

The recommendations for remediating the risks and vulnerabilities found are described in the following table**.**

Risks and Recommendations

Risk	Risk Level (Critical, High, Moderate, Low)	8.1 Admin Office Recommendations
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	High	Medicaid databases should be up to industry standards. Using the MECT ver, 2.3
4	Moderate	Renew HIPAA server licensing.
5	Critical	Determine legitimacy of the breach. Fix all potential loopholes and discover any possible compromised information and/or machines. Strongly recommend Anti-Viral scan on all machines to ensure company security. Possible breach should be kept on a need-to-know basis.
6	High	Fully establish all the partially completed SSPs. The SSPs must contain all necessary features in the event of a security breach.
7	Critical	Create and implement SSPs for all assets without one as soon as possible.

8	High	Ensure that employees secure all patient data when they are not directly using it.
9	Critical	Establish a Disaster Recovery Plan for all assets without one as soon as possible.
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.2 Facilities Office Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	High	Develop and deploy a baseline for all machines in the department. Ensure that they are secure, all programs and drivers are up to date, and they have all security programs installed and active.
4	High	Fully establish all the partially completed SSPs. The SSPs must contain all necessary features in the event of a security breach.
5	Moderate	Service level agreements need to be drafted and delivered to all relevant employees, suppliers, and customers.

Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.3 Pharmacy Office Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	Critical	Update policies on account creation and termination. Accounts that are inactive for 90 days must be removed. New employees must be trained on how to access their data correctly. Employees should be taught basic account safety rules like not sharing passwords and logging out when they are finished. Assign staff from IT department to monitor account activities and teach employees.
4	High	Fully establish all the partially completed SSPs. The SSPs must contain all necessary features in the event of a security breach.
5	Critical	Create and implement SSPs for all assets without one as soon as possible.
6	High	Ensure that employees secure all patient data when they are not directly using it.
7	Moderate	Service level agreements need to be drafted and delivered to all relevant employees, suppliers, and customers.
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.4 Dental Department Recommendations**

1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	Critical	Update policies on account creation and termination. Accounts that are inactive for 90 days must be removed. New employees must be trained on how to access their data correctly. Employees should be taught basic account safety rules like not sharing passwords and logging out when they are finished. Assign staff from IT department to monitor account activities and teach employees.
4	High	Develop and deploy a baseline for all machines in the department. Ensure that they are secure, all programs and drivers are up to date, and they have all security programs installed and active.
5	Critical	Create and implement SSPs for all assets without one as soon as possible.
6	High	Ensure that employees secure all patient data when they are not directly using it.
7	Critical	Establish a Disaster Recovery Plan for all assets without one as soon as possible.
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.5 HR Department Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	Moderate	Renew HIPAA server licensing.
4	High	Test all employees for comprehension on HIPAA. This test should be broken down into several sections that assess specific regulations. Staff will take a class for each section they failed/performed poorly on. Staff will continue to take the test and go to class until they pass. Staff will have to test and retrain annually.
5	High	Fully establish all the partially completed SSPs. The SSPs must contain all necessary features in the event of a security breach.
6	Critical	Create and implement SSPs for all assets without one as soon as possible.
7	Moderate	Service level agreements need to be drafted and delivered to all relevant employees, suppliers, and customers.
8	Critical	Suspend access to sensitive information from all staff that have not had a background check. Interview staff over troubling findings and take appropriate action based on the results of the background checks.
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.6 Business Office Recommendations**

1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	High	Medicaid databases should be up to industry standards. Using the MECT ver, 2.3
4	Moderate	Renew HIPAA server licensing.
5	High	Fully establish all the partially completed SSPs. The SSPs must contain all necessary features in the event of a security breach.
6	Critical	Create and implement SSPs for all assets without one as soon as possible.
7	High	Ensure that employees secure all patient data when they are not directly using it.
8	Moderate	Service level agreements need to be drafted and delivered to all relevant employees, suppliers, and customers.
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.7 Audiology Office Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	High	Develop and deploy a baseline for all machines in the department. Ensure that they are secure, all programs and drivers are up to date, and they have all security programs installed and active.
4	Critical	Update policies on account creation and termination. Accounts that are inactive for 90 days must be removed. New employees must be trained on how to access their data correctly. Employees should be taught basic account safety rules like not sharing passwords and logging out when they are finished. Assign staff from IT department to monitor account activities and teach employees.
5	Critical	Create and implement SSPs for all assets without one as soon as possible.

6	Moderate	Service level agreements need to be drafted and delivered to all relevant employees, suppliers, and customers.
7	Critical	Establish a Disaster Recovery Plan for all assets without one as soon as possible.
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.8 Radiology Department Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.

3	High	Develop and deploy a baseline for all machines in the department. Ensure that they are secure, all programs and drivers are up to date, and they have all security programs installed and active.
4	Critical	Update policies on account creation and termination. Accounts that are inactive for 90 days must be removed. New employees must be trained on how to access their data correctly. Employees should be taught basic account safety rules like not sharing passwords and logging out when they are finished. Assign staff from IT department to monitor account activities and teach employees.
5	Critical	Create and implement SSPs for all assets without one as soon as possible.
6	High	Ensure that employees secure all patient data when they are not directly using it.
7	Critical	Establish a Disaster Recovery Plan for all assets without one as soon as possible.

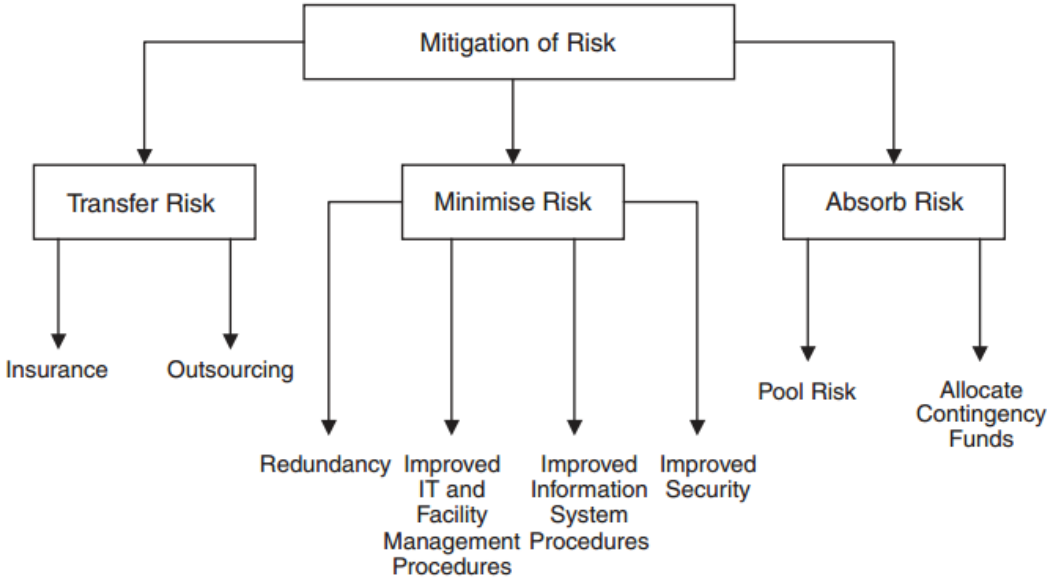
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.9 Pediatrics Department Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	High	Develop and deploy a baseline for all machines in the department. Ensure that they are secure, all programs and drivers are up to date, and they have all security programs installed and active.
4	Critical	Update policies on account creation and termination. Accounts that are inactive for 90 days must be removed. New employees must be trained on how to access their data correctly. Employees should be taught basic account safety rules like not sharing passwords and logging out when they are finished. Assign staff from IT department to monitor account activities and teach employees.
5	Critical	Create and implement SSPs for all assets without one as soon as possible.
6	High	Ensure that employees secure all patient data when they are not directly using it.
7	Critical	Establish a Disaster Recovery Plan for all assets without one as soon as possible.

Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.10 Lab Department Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.

3	High	Develop and deploy a baseline for all machines in the department. Ensure that they are secure, all programs and drivers are up to date, and they have all security programs installed and active.
4	Critical	Create and implement SSPs for all assets without one as soon as possible.
5	High	Ensure that employees secure all patient data when they are not directly using it.
6	Moderate	Service level agreements need to be drafted and delivered to all relevant employees, suppliers, and customers.
7	Critical	Establish a Disaster Recovery Plan for all assets without one as soon as possible.
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.11 Mental Health Department Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	High	Develop and deploy a baseline for all machines in the department. Ensure that they are secure, all programs and drivers are up to date, and they have all security programs installed and active.
4	High	Fully establish all the partially completed SSPs. The SSPs must contain all necessary features in the event of a security breach.
5	Critical	Create and implement SSPs for all assets without one as soon as possible.
6	High	Ensure that employees secure all patient data when they are not directly using it.
7	Moderate	Service level agreements need to be drafted and delivered to all relevant employees, suppliers, and customers.
8	Critical	Establish a Disaster Recovery Plan for all assets without one as soon as possible.
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.12 Food Services Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	High	Develop and deploy a baseline for all machines in the department. Ensure that they are secure, all programs and drivers are up to date, and they have all security programs installed and active.

4	Critical	Update policies on account creation and termination. Accounts that are inactive for 90 days must be removed. New employees must be trained on how to access their data correctly. Employees should be taught basic account safety rules like not sharing passwords and logging out when they are finished. Assign staff from IT department to monitor account activities and teach employees.
5	Critical	Create and implement SSPs for all assets without one as soon as possible.
6	Critical	Establish a Disaster Recovery Plan for all assets without one as soon as possible.
7	Low	Establish a documented vendor plan so that food suppliers can supply the correct food for patients with specific dietary needs.
Risk	**Risk Level (Critical, High, Moderate, Low)**	**8.13 Information Technology Department Recommendations**
1	High	Passwords should contain at least 12 characters and shall not have any dictionary words or names. Passwords shall be reset every 60 days at most.
2	Moderate	Branches should get together to determine a standard for communication.
3	Critical	Apache Struts shall be updated on all machines immediately. Investigate any possible breaches and/or exploits through Apache Struts. Continue to update regularly to ensure security.
4	High	To comply with HIPAA regulations, logs shall be kept for at least 6 years.
5	Moderate	Renew HIPAA server licensing.
6	Critical	Determine legitimacy of the breach. Fix all potential loopholes and discover any possible compromised information and/or machines. Strongly recommend Anti-Viral scan on all machines to ensure company security. Possible breach should be kept on a need-to-know basis.
7	Critical	To comply with HIPAA regulations, encryption is to be applied to all data when it is assessed to be appropriate. Sensitive data including patient health data and other secure information must be sent through a layer of security. SSL will no longer be used unless the clinics can communicate through an intranet or they encrypt all data being sent.
8	Critical	All wireless access points on the WLAN must be secured by requiring a password. All unidentified devices on the WLAN must be removed and blacklisted unless it is deemed safe. Active logging and network monitoring will be implemented to prevent any unexpected connections.
9	High	Fully establish all the partially completed SSPs. The SSPs must contain all necessary features in the event of a security breach.
10	Critical	Create and implement SSPs for all assets without one as soon as possible.
11	Moderate	Service level agreements need to be drafted and delivered to all relevant employees, suppliers, and customers.

12	High	Escalation path needs to be introduced so that issues can be brought up to the appropriate manager. This will both speed up operations and prevent large scale breaches.
13	Critical	Establish a Disaster Recovery Plan for all assets without one as soon as possible.



Risk Management Budget Plan

Budget recommendations for the next 3 fiscal years

This budget recommendation was creating with the biggest flagged risks in mind. One of the biggest information insurance risk identified were the employees not being update on policies, laws, and regulation that they need to follow then handling patient data or hospital technology in general. Due to this we advise spending at least $750,000 on Deloitte Advising for them to come out and regularly train the hospital employees and perform workshop session. The second biggest spending area that we advise is networking and cloud security. Since the hospital has two off site clinics and the patients can access their information from home, a lot of data must be stored in the cloud and adequately protected during transfer.

> Mission: “Providing right on time healthcare to clients while enabling the customers.”
>
> Vision: Providing ubiquitous and secure mobile access to patients through patient portals to enable preventive medicine through transparency.”

Because of those risk and the mission statement of providing on time healthcare, we advise investing in cloud security services to allow safe and quick access for patients and staff while ensuring maximum security and risk identification & mitigation. On top of that this budget is highly customizable in the future. So once risk has been brought down to an acceptable & manageable level you can look at transferring funds to a different risk that either needs more resources or funding. Another huge area of the budget should always be reserved for audit. As of this risk assessment, we recommend an HIPPA and general personal data Audit to make sure you are in compliance with all laws and regulation. Also, having multiple sets of eyes from different organization looking at your process can help identify risk that might have been missed during a first audit or analysis.

Item	Department	Owner	Cost
Data Leak Prevention	IT	Udolph Schwarz	$270,000
Cloud SOC	IT	Collby Fraley	$75,000
AntiVirus McAfee	IT	Karley Wilkins	$35,000
Symentic ICDx	IT	Kimbel Burrows	$28,000
Palo Alto Firewall	IT	Deacon Booker	$80,000
Aruba Networks	IT	Deacon Booker	$5,000
Deloitte Training	IT	Udolph Schwarz	$750,000
Infoblox	IT	Udolph Schwarz	$24,000
Qualys	IT	Collby Fraley	$25,000
Recommind	IT	Jaden Newton	$2,500
Splunk	IT	Kimbel Burrows	$150,000
AlertLogic	IT	Humberto Lin	$45,000
Cisco ISE	IT	Deacon Booker	$50,000
Office 365 Enterprise	IT	Udolph Schwarz	$150,000
Crowdstrike	IT	Jaden Newton	$8,500
FireMon	IT	Kimbel Burrows	$20,000
Tanium	IT	Karley Wilkins	$5,000
Tenable	IT	Collby Fraley	$60,000
VMware	IT	Kimbel Burrows	$8,000
EHR	Admin Office	Benvolio Mein	$28,000
Netgain EHR hosting	IT	Jaden Newton	$10,000
Salesforce	IT	Collby Fraley	$10,000
Azure cloud storage	IT	Humberto Lin	$25,000
Red team Pen test	IT	Collby Fraley	$250,000
HIPPA Audit	IT	Udolph Schwarz	$100,000
Employee Audit	IT	Humberto Lin	$75,000
Cloudscan	IT	Kimbel Burrows	$20,000
Physical Security	IT	Udolph Schwarz	$250,000
OneTrust Data Guidance	IT	Kimbel Burrows	$175,000
TOTAL:			$2,979,000

Incident Handler/Incident Response

In the event of an incident, it is paramount to ensure that there are a clear set of rules and guidelines to follow. It is also extremely important to set up a chain of command and establish who should oversee the handling of any potential incidents.

Incident Handler

Depending on the departments that have been affected, all noticed incidents need to be reported to the immediate managing staff and then relayed to the department head, as well as the head of IT. Department Heads will have a better grasp of who is affected directly and can move staff around to solve issues quickly. On top of advising superior staff, the staff and manager who first noticed the incident should write a report detailing the exact substance of the incident, when it was first noticed, and a list of infected machines, programs, or other computer related items.

Incident Response

The incident response shall follow 5 steps to ensure that all damage incurred is kept to a minimum, protecting both the employees and patients involved.

1. Preparation – To prevent and/or catch incidents early, it is necessary to keep all security programs and software up to date. Staff should also know exactly what to do and who to call if such an emergency should occur.
2. Identification – The IT department should immediately look at the written report submitted by the first exposed staff to help determine what the incident may entail. In addition to this, on site testing should be done, as well as interviews if they are necessary and relevant to the issue on hand.
3. Containment – IT staff should work to isolate the infected machines, programs, and other computer related items that may have been infected to slow down and stop the spread of any potential infections. This might look like shutting down internet services or unplugging a device.
4. Eradication – Once the containment is successful, eradication of the threat is necessary to prevent further issues. In some extreme cases entire computers will be damaged beyond repair. It is safer to err on the side of caution than miss the threat and fail to eradicate it.
5. Recovery/Lessons Learned – Once the threat has been neutralized the IT department should work with the infected department to find all data that might have been lost, damaged, or stolen in the incident. Also, all issues noted in the identification phase must be addressed. If a staff member clicked a phishing link, **all** staff should be required to take at least one course on phishing. If a driver or program is found to be out of date, the IT department should move to patch the vulnerable machines as soon as possible.

In handling incidents communication and cooperation is key. The preparation phase of incident handling should be on going to continuously work towards a better information assurance policy for the company and its patients. Incident handling is also important to achieve secure access and timely healthcare in accordance with both the mission and vision of the company.

Information Assurance Overall Recommendations:

The overall recommendations for MMC are represented in the following table.

Information Assurance Overall Recommendation for MMC

Vulnerability for Testing	**Remediation**
Only one form of authentication is used to access the systems.	Use a system of Multi-Factor authentication such as biometrics or a card system that will implement something
Passwords are changed only every 6 months and require an 8-character minimum	Require that the password length be extended by and extra four characters and the passwords need to be updated in the system once every 60 days.
There are several accounts that have been abandoned, several of those accounts were from employees that were fired within the last 6 months	Make sure that the accounts of all employees that were terminated have been deactivated.
Several Patches of Apache Struts are missing in the system	The system should be updated and managed to make sure that updates are automatically updated and checked for integrity.
There are no configuration baselines for 8 systems	All systems should have baselines for their critical software. In the company policy jacket, there should be an incorporation of baselines to control manage each system.
Logs are being overwritten every two years	All logs older than 2 years should be kept in a database where it can be acquired at later times. Also the logging system should delete the program for overwriting data
Medicaid Database is not adequately secured	Since this not only deals with PII but also patient insurance information, security systems need to put in place to make sure that only authorized personnel may access the information.
Scope Creep for several Long term employees who had changed roles	With scope creep, there should always be some sort of Access Control in place whether it be MAC, RBAC or DAC. These will eliminate the issues of scope creeping
Scans showed that several of the critical risks had vulnerabilities	These need to be addresses immediately and with proper assurance to the assets. Risk analysis should be ran every quarter to ensure that vulnerabilities are being mitigated

HIPPA Server is at the end of its life cycle	Prior to the end of any servers life cycle, the company should have a plan to discuss about the next action to take with the CIO about the servers that hold information regarding patient data and HIPPA records and policies.
Vulnerability for Interviews	**Remediation**
HIPPA training is not consistent throughout all departments	In the policy Jacket it should be disclosed that HIPPA and other trainings are mandatory for all employees and future employment is contingent on that training being complete.
Employees often left patient records on their desks	As part of the security protocol, after records have been viewed, if not being actively worked on all patient records and files need to be locked up and kept in a secure place until needed again.
HIPPA RA was done 5 years ago, but nothing followed or was documented.	All RA need be documented and kept for records as well as the CIO and other security personnel need to follow through with assessment protocols on mitigating vulnerabilities.
Management was not focusing on the security measures of the organization	A top down approach would best suit the need for higher level management to be actively involved in the security process and allow for employees to see its importance.
A third of the employees interviewed did not know what HIPPA was.	All employees must go g=through a training seminar at least once a year, refreshing information on the HIPPA rules and regulations that must be followed.
Employees spoke of a breach that was Bit Reported	Breaches in security are supposed to be disclosed when needed, however there should be policies in place to make sure that speaking of breaches in a certain light should be prohibited.
Employees did not know who to contact in case of a breach.	In the policy jackets all employees should know who to contact in in what manner of time frame in case of a breach.
Patients and employees can print medical documents from home	If PII and other medical documents are required to be printed from home, there needs to be a VPN portal to allow access to those documents in a secure fashion.

Remote hospital is still using SSL to send sensitive data to the main hospital.	All information needs to be sent over a secure protocol such as HTTPS or DNS preferably in order to mitigate risk of breach or exposure
Remote access point allows for rouge devices to logon	All remote access points should only allow those with authorized credentials to logon to the network.
Vulnerability for Documentation	**Remediation**
At least half of the assets have no System Security Plan	All departmental assets need to have a security plan in place so that the assets in question can be properly protected
The assets with SPP are missing pertinent information such as flowcharts and classifications	All departmental assets need to have a risk and asset classification is done at least once every year in order to help with the security protocols. Make sure that all information is properly documented as well.
1/3 of the assets have no Disaster recovery plan	All assets and documentation must have a Disaster recovery plan and that plan should be evaluated once every quarter to ensure that in case of failure to prevent disaster, the plan still works.
1/10 of the Employees have outdated computer behavior rules	As part of their on boarding training and continued education, all employees should have to go through proper computer training
Background checks for several Vendors have not been done	All vendors must have background checks done before being allowed to work with the organization. Policies should include methodology to background checks.
There were several missing policies for provisioning, deprovisioning, orientation and termination.	All policies for employee introduction and termination for the company should be well documented and all employees should know the provisions for employment and termination.
Several vendor service agreements have been missing	Before allowing partnership with the organization, all vendors must fill out and sign a service level agreement which should be kept with the department records for keeping.

The cloud providers have not and do not offer a path for problem escalation.	The organization should make sure to partner with an IaaS that will allow for problem escalation and service requests for all issues.
There is no documented vendor management plan	As stated in the policy jacket management plans for the vendors must be documented and kept for at least 5 years so that all plans may be kept in order from time of inception.
There is no MOU, however there is several interconnected systems.	A memorandum of understanding is a document that describes the broad outlines of an agreement that two or more parties have reached. All of those systems should have a place in the MOU to make sure that all of the systems have a well-documented summary.

Many of the assets in this organization or of the moderate to critical level and above, however the organization has not used sufficient measures to ensure that those assets are properly secured. Recommendation needs to implement within reason effective immediately in order to mitigate and legal and other social consequences. The following recommendations should be taken into account in order to preserve MMC's mission of providing right on time healthcare to clients while enabling customers as well as MMC's vision of providing ubiquitous and secure mobile access to patients through patient portals to enable preventive medicine through transparency.

Works Cited

Benefield, H., Ashkanazi, G., & Rozensky, R. H. (2006). Communication and records: HIPPA issues when working in health care settings. *Professional Psychology: Research and Practice*, *37*(3), 273–277. https://doi.org/10.1037/0735-7028.37.3.273

Kremling, J., & Sharp Parker, A. M. (2018). *Cyberspace, cybersecurity, and cybercrime*. Los Angeles, CA: SAGE.

Qian, Y., Tipper, D., Krishnamurthy, P., & Joshi, J. (2010). *Information Assurance: Dependability and Security in Networked Systems*. Morgan Kaufmann.

Schou, C., & Hernandez, S. (2015). Chapter 10. In *Information assurance handbook: Effective computer security and risk management strategies* (pp. 101-109). New York, NY: McGraw-Hill Education.