Premium Health Risk Management Plan

CYB 411-Summer 2019

Gagneet Sahota

2019

# Introduction

## Mission

The mission of information technology security is to protect critical information resources that support Premium Health, to exchange information with its patients, allow online bill to pay and allow an online directory to better serve its patients.

## Project Goal

The goal of this risk management process is to protect Premium Health and its ability to operate and to help patients. But also to have policies in place to protect the confidentiality, integrity and availability of data stored/ transmitted.

## Purpose

The purpose of a risk management plan is not to eliminate all risk, but rather to keep risk at a level where protection failures are within anticipated and acceptable ranges. The security risks associated with healthcare service organizations have increased as technology and networking has grown. With more ways to communicate and help patients, the list of risks always increases more than any organization can afford to fully eliminate. The process for managing healthcare systems IT security-related risks is very similar to the HIPAA standards that the industry has been following. This paper recommends that similar methods be applied to any IT security risks to healthcare service systems.

## Objectives

Specific objectives of this project’s Risk Management Plan include:

* Ensure critical risks impacting scope, performance of the organization, budget, or change to management are identified, communicated, mitigated, and escalated in a timely manner.
* Facilitate attention to important risks impacting the project and the organization.
* Produce meaningful information that allows project management to focus efforts on the important risk that may have a high impact on business operations.
* Ensure appropriate stakeholders are informed and, if applicable, participate in the mitigation.

## Scope

The Premium Health system must be maintained to the federal mandate of HIPAA or it can be subject to penalties and loss of customers. Unauthorized changes to data, production outages and other problems such as loss of data can lead to the loss of credibility and dependability of the health organization. This paper uses known threats from the previous risk management plan on file to develop a new risk management plan for Premium Health. The current known threats with others are stated in the risk assessment plan.

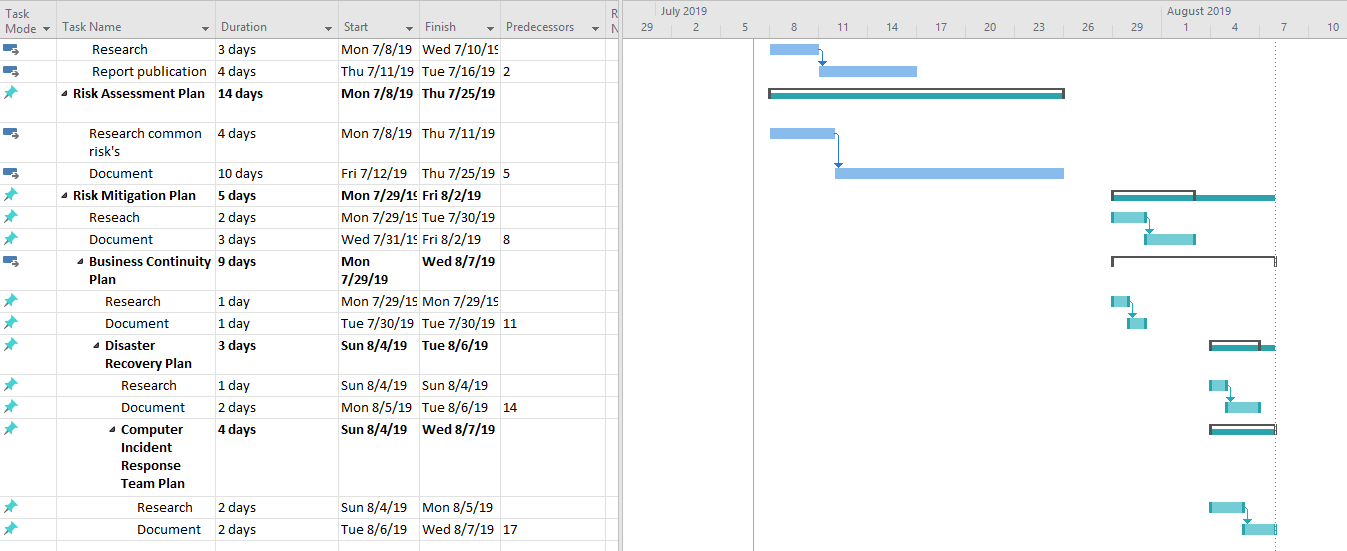
## Compliance laws

* HIPAA Security Rule- All data needs to be confidential, have integrity and available of all ePHI. Premium Health needs to identify and protect against reasonably anticipated security threats that may compromise ePHI. The organization also needs strong logs of accessed information to prevent unauthorized uses or anticipated mishandling. For the physical aspect, the organization should have control of who can have physical access to the servers where the data is stored. Also have strong user authentication so potential malicious users can’t access workstations. The technical aspect, Premium health needs to have audit controls in place to review that data doesn’t lose its integrity through the process in place.
* HIPAA Privacy Rule- Premium Health needs to have strong disclosures for authorization to share PHI. And strong user authentication to prevent patient health records becoming comprised under any attack to the user or organization.
* HIPAA Enforcement Rule- If a breach were to happen, Premium Health should have a string system in place to notify those that were affected by the breach by HIPAA standards.
* PCI DSS Security standards- The PCI DSS security standards are in place for organizations that handle any type of card payments. 1 through 12 will apply to Premium Health because of the online portal that accepts card payment from patients.

**1.7 Roles and Responsibilities**

* CEO- The Chief Officer has an overall responsibility to ensure there is an updated risk management plan in place and infrastructure to support the plan to minimize risk to the organization. The CEO also has the duty to delegate specific roles and responsibilities to senior management to ensure the risk management plan is coordinated.
* Senior management- The expected responsibility is to ensure risks are appropriately identified and controlled. And to support the risk management plan with resources ,whether that be new equipment funding needed or to educate employees for safe security practices.
* Staff of Premium Health- Understand the risk stated in the risk management plan and provide feedback on different training methods to lower risk. The staff will also be responsible of finding what the cost of outages or data that will be lost if an outage occurs.
* HR – Work with the IT security team to deliver new training of best practices for the system. Inspecting all data sources to make sure it follows HIPAA such as how data is protected, stored and transmitted. And a list of cost associated with noncompliance.
* Chief Information Officer- The CIO will be responsible for budgeting and planning for the Premium Health IT department. And also identifying possible threats, vulnerabilities, recommended solutions and the cost to these solutions.
* IT Department- The IT department will need to work with the CIO to implement proper security practices and be complaint with all data regulations. And help identify new threats and vulnerabilities on the user level.
* Director of Finance for Premium Health- The Director of finance has the responsibility to ensure that the system is in compliance with the PCI DSS requirements. And to minimize any additional financial risk that may be discovered.

# 1.8 project Schedule



# Risk Assessment Plan

**Scope**

The Risk assessment plan will evaluate services like PMCare, PMPay and PMNet to ensure the data and physical servers are in HIPPA/ PCI DSS compliant. The scope of this project will include any physical, procedural, and technical controls related to the webservers, database servers that host these online services and the 300 company owned devices. This risk assessment plan will analyze both locations that Premium Health operates, and the procedure controls of the servers located in AWS.

**Purpose**

The purpose of performing a risk assessment is to identify and evaluate any potential threats and vulnerabilities in the Information System of Premium Health. When threats are identified, they will be analyzed to find the impact and probability the threat will occur. Then based on the risk level of the identified threats, appropriate controls will be suggested to mitigate or reduce the threat from occurring. This will help the organization understand where risks exist, and how much level of risk the organization is willing to accept. It will also look at current controls in place to see if they are effective.

**Importance**

It is important to conduct a risk assessment to protect the current infrastructure against any attacks. Without having a proper risk assessment done to the system it is hard to be sure that the system is keeping patient data safe and confidential. The risk assessment will not only save money to the organizations by ensuring there are countermeasures for an outage but will also increase the confidence of its patients/ customers in Premium Health.

**Approaches**

There are two common approaches when performing a risk assessment:

* **Quantitative-** Unlike the qualitative method, the quantitative method uses predefined formulas. To use the formula, you will need to collect data about the threats or events that have taken place or may take place. If a single incident has occurred, this would be a single loss expectancy and would be expressed using how much the incident cost the organization. An annual rate of occurrence is the number of times you expect the incident to take place in a year. And to find the Annual loss expectancy, you would multiply the SLE x the ARO. This formula helps make an informed decision when implementing a new safeguard control, as if the control is less than the ALE, it is easier for management to see the benefit and approve the purchase.
* **Qualitative –** Another approach is the qualitative method, which is the method to use when one doesn’t have access to the data required for the quantitative method. The qualitative method is just as effective as it uses the opinions of experts to determine the probability that the risk will occur and the impact of the risk if it was to occur. This method helps you prioritize the most important risk to the least important.

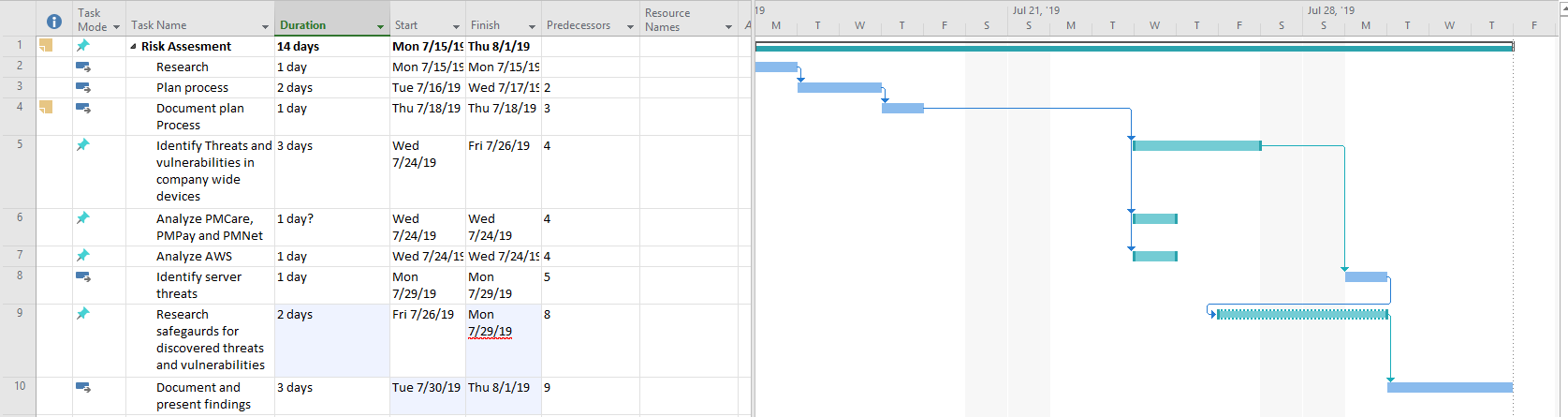
**Outline**

* Will cover any threats or vulnerabilities found on the laptops and workstations via hardware or software.
* Will identify any physical threats to the server’s location causing it to go offline
* Asses any potential natural disasters that many occur in Klamath falls or in Portland that would affect the availability of the system.
* Identify any software related vulnerabilities to the web servers hosting PMCare, PMPay and PMNet.
* Identify any vulnerabilities in the way data is transmitted to and from the AWS servers.
* Identify any vulnerabilities in the method the data is accessed by authorized users.
* Ensure all cardholder data related to PMPay is up to PCI DSS standards
* Identify any technical or procedural threats or vulnerabilities when handling data related to PMCare, PMPay and PMNet.
* Find safeguards to the threats/ vulnerabilities identified.

**Roles and Responsibility’s**

* Senior management- The expected responsibility is to make informed decisions on controls to keep the organization safe from threats and vulnerabilities. And with the help of IT, natural disaster risk’s will be assessed. Senior managements role in the risk assessment will be to make the decision of how much risk the organization wants to be exposed to and based on the research provided, which controls to implement.
* Accounting Department – The accounting department will be expected to review the checklist of PCI DSS standards to see if they comply with the standards and document which requirements they do not comply with. Accounting role will be to provide documentation to IT to identify if any threats or vulnerabilities exist related to PMPay or the procedure of handling cardholder data.
* IT Department- IT will be responsible for identifying any threats or vulnerabilities that exist on the 300 devices in Premium Health. IT will also be responsible analyzing the server locations at both Premium Health in Klamath and Portland to ensure no unauthorized access is available to the servers. And will observe working conditions in the work place to identify additional procedural and technical risks.
* Nursing Staff- Assuming the nursing staff enters patient data into PMCare, the nurses will be responsible for documenting the current method of data entry. The nurses will also assist IT with any questions that rise over current procedural methods.

**Schedule**



# Risk Mitigation Plan

* **Control**- Windows Server 2019

Description- The latest version of Windows Server to upgrade the Portland location servers.

Purpose – Upgrade the four servers currently running Windows Server 2008 before end of life to keep servers patched and secure.

Implementation plan- Due to the severity of the risk and time till end of life for updates this will need to be implemented immediately. This will be implemented on a Friday night to avoid interruptions in workflow as this is assumed the slowest time for business operations. Each server will be taken off one at a time to avoid loss of data.

Timeline for implementation – Will be implemented immediately once cost is approved by senior management.

Test plan- Before the upgrade takes place, the new version will be installed on to a sample server with the services/application running on the current servers to ensure all the hooks/process are function correctly before implementing in a live environment.

Cost- Due to the user count and what the servers will be handling, the Standard edition was chosen a best fit for the organization. The cost for one license is $972, and four will be needing to upgrade the servers running the 2008 version, equaling $3,888.

* **Control**- Windows update

Description- To avoid the CVE-2018-8410 and CVE-2014-4072 vulnerability the server will need the 4343901-patch along with the latest version of .NET framework installed.

Purpose – Upgrade the three servers currently running unpatched by the CVE-2018-8410 and CVE-2014-4072 vulnerability.

Implementation plan- Due to the severity of the risk and time till end of life for updates this will need to be implemented immediately. This will be implemented after hours as it will just need to be sent out via active directory and may require a restart for the servers.

Timeline for implementation – Will be implemented immediately once as the risk severity is high.

Test plan- Before the update takes place, the new version will be installed on to a sample server with the services/application running on the current servers to ensure all the hooks/process are function correctly before implementing in a live environment.

Cost- Since the server is still in the product cycle windows updates will be free. The only real cost will be the labor to install the updates and test the servers after.

* **Control**- Disaster Recovery Plan review

Description- A review of the detailed plan to get Premium Health back running after a potential threat.

Purpose – To ensure the organization can resume business quickly and effectively in case of a disaster.

Implementation plan- Due to the severity of the risk this will need to be implemented immediately.

Timeline for implementation – The review of the disaster recovery plan will happen after the approval of senior management for a day where they can be present in the review process.

Test plan- After the plan has been reviewed, it will be tested in a test environment to ensure it is still effective.

Cost- The only real cost will be the labor to review the disaster recovery plan and test if it still is up to date with hardware already provided.

* **Control**- Electronic Door lock

Description- A door lock that uses RFID cards to unlock and secure important rooms.

Purpose – To ensure the organization can preserve confidentiality integrity and availability of its data the lock will be placed on the Telco closet with restricted access.

Implementation plan- Due to the severity of the risk this will need to be implemented immediately after approval of cost by senior management.

Timeline for implementation – Once approval has been attained by senior management.

Test plan- Lock will be tested to ensure only those who have the RIFD cards will be able to access the telco closet.

Cost- The cost will be around $250 for the install of the lock and price of the lock.

**Location**: Klamath Falls, Oregon

* **Control**- GreCon Smoke detector

Description- A smoke detector that can sense fine smoke particles

Purpose – To trigger the fire suppression system when smoke is detected to prevent fire and data loss.

Implementation plan- Due to the severity of the risk this will need to be implemented immediately after approval of cost by senior management.

Timeline for implementation – Once approval has been attained by senior management.

Test plan- Once installed, the annual test will be conducted again to ensure it is in working order.

Cost- The cost will be around $550 for the install of the detector

* **Control**- Transfer of Data and erase data on Backups

Description- Transfer CAV2/CVC2/CVV2/CID data from primary payment processing server to more secure server. And delete backups that contain CAV2/CVC2/CVV2/CID data

Purpose – To avoid breaches CAV2/CVC2/CVV2/CID should not be stored on the same server as the payment processing.

Implementation plan- Due to the severity of the risk this will need to be implemented immediately after approval of procedure by senior management.

Timeline for implementation – Once approval has been attained by senior management.

Test plan- Process a payment and see if the data is stored on the payment processing server.

Cost- The cost will be labor hours of IT transferring data and configuring the payment processing server to transfer to another server on site.

* **Control**- Locked storage closet

Description- Have a storage closet with a secure lock built for IT department.

Purpose – To avoid breaches or tampering to any hardware/data, a storage closet will be made to store production server hardware.

Implementation plan- Due to the severity of the risk this will need to be implemented immediately after approval of cost by senior management.

Timeline for implementation – Once approval has been attained by senior management.

Test plan- Once the closet has been made ensure the closet is secure and has proper HVAC to ensure climate control.

Cost- The cost for the closet with the secure lock and an extension of the current HVAC system will be $15,000.

* **Control**- Upgrade to Cisco IOS 15.5

Description- Will upgrade the Cisco 6800 switches to the latest version available.

Purpose – To patch the vulnerability found in the IOS 15.1 release.

Implementation plan- During a Friday night the switch will be upgraded to avoid interruptions to business operations.

Timeline for implementation – Once approval has been attained by senior management.

Test plan- Once the switch is upgraded, it will be tested to ensure the vulnerability isn’t still present.

Cost- Since the switch is still in the product cycle for Cisco, it will be free. The only real cost will be the labor to install the updates and test the switches after.

* **Control**- Create Policy for relived user accounts

Description- When an employee leaves or is on vacation this policy will be implemented to ensure all data remains secure.

Purpose – To avoid any breaches or threats by inactive user accounts.

Implementation plan- A policy will be created and then sent to the senior management for approval.

Timeline for implementation – Once approval has been attained by senior management.

Test plan- Test a user account that has been disabled to see if the user can still login after considered disabled

Cost- The only real cost to implement will be for creating policy and implementing policy organization wide.

* **Control**- Windows update

Description- To avoid CVE-2017-11935vulnerability the server will need the latest windows updates.

Purpose – Upgrade the workstations currently running excel version that’s includes the CVE-2017-11935 vulnerability.

Implementation plan- Due to the severity of the risk and time till end of life for updates this will need to be implemented immediately. This will be implemented after hours as it will just need to be sent out via active directory and may require a restart for the workstations.

Timeline for implementation – Will be implemented immediately as the risk severity is high.

Test plan- Before the update takes place, the new version will be installed on to a sample workstation with the services/application running on the current workstations to ensure all the hooks/process are function correctly before implementing in a live environment.

Cost- Since the workstations excel version is still in the product cycle windows updates will be free. The only real cost will be the labor to install the updates and test the workstations after.

# Business Impact Analysis Plan

**PMPay**

Premium Health provides many services, including PMPay which is the primary source of income for the company as it’s the system to take payments from patients. First, we will conduct a Business Impact Analysis on PMPay to uncover what would be needed in case of a business emergency, to continue daily business operations.

Because users need to be able access PMPay.com for users to pay their bill and Premium Health to gain revenue. The process is the flowing to identify the critical business functions:

* User will need to access PMPay
* Web server will need to be able to communicate with the payment server

Next, we’ll look at the critical resources needed for the critical business functions identified above to operate. Because both functions are related to technology hardware, they share most of the same critical resources. To run PMPay the critical resources are web servers, HVAC system, a firewall and electrical. If any of the critical resources identified were to fail, it could potentially stop PMPay from running normally.

Third we’ll look at the maximum acceptable outage and impact of an outage of any CBF for PMPay. An outage of CBF #1, would have a high impact on users able to view/pay their bill. Hence the MAO should be less than 10 minutes of downtime. Although CBF #2 also has a high impact as users won’t be able to submit their payment if the communication between servers is down, most users will still be able to view their bill. So, the MAO for CBF #2 can be a little more as in 15 minutes of downtime as users will still have to return to the site to pay their bill. Based on the information gathered the recovery priority will be to ensure users are able to access PMPay and ensure that critical resources of web servers and electrical are priority in the recovery process.

**PMCare**

Another key service is PMCare which allows patients, doctors, clinics and customers to communicate with each other. Because users need to be able access PMCare for users to communicate with its doctors and obtain results, it is critical to conduct a Business Impact analysis on the service. The process is the flowing to identify the critical business functions:

* Users will need to access PMCare portal
* Web server will need to be able to communicate with the location server

Next, we’ll look at the critical resources needed for the critical business functions identified above to operate. Because both functions are related to technology hardware, they share most of the same critical resources. To run PMCare the critical resources are web servers, HVAC system, a firewall and electrical. If any of the critical resources identified were to fail, it could potentially stop PMCare from running normally.

Third we’ll look at the maximum acceptable outage and impact of an outage of any CBF for PMCare. An outage of CBF #1, would have a high impact on users able to view/respond to messages. Hence the MAO should be less than 5 minutes of downtime as doctors and clients share critical information this platform. Although CBF #2 also has a high impact as users won’t be able to communicate with doctors, they’ll be able to access the portal and view previous messages/test results. So, the MAO for CBF #2 can be a little more as in 10 minutes of downtime as users will still have to return to the site to see a response from the other user. Based on the information gathered the recovery priority will be to ensure users are able to access PMCare and ensure that critical resources of web servers and electrical are priority in the recovery process.

**PMNet**

The last service is PMNet which allows patients, doctors, clinics to view information about the Premium Health network. Because users need to be able access PMNet for patients to find doctors to treat them, it is critical to conduct a Business Impact analysis on the service. The process is the flowing to identify the critical business functions:

* Users will need to access PMNet directory
* Doctors will need to be able to login to update info

Next, we’ll look at the critical resources needed for the critical business functions identified above to operate. Because both functions are related to technology hardware, they share most of the same critical resources. To run PMNet the critical resources are web servers, HVAC system, a firewall and electrical. If any of the critical resources identified were to fail, it could potentially stop PMNet from running normally.

Third we’ll look at the maximum acceptable outage and impact of an outage of any CBF for PMNet. An outage of CBF #1, would have a medium impact on users able to view/find doctors in the Premium Health network resulting in lower revenue. Hence the MAO should be less than 15 minutes of downtime as new patients won’t be able to contact doctors. CBF #2 also has a medium impact as doctors wont be able to update their information but others will be able still view it. So, the MAO for CBF #2 can be a little more as in 30 minutes of downtime as doctors can update the sit later or inform the patient over the phone when they call. Based on the information gathered the recovery priority will be to ensure users are able to access PMNet and ensure that critical resources of web servers and electrical are priority in the recovery process.

# Business Continuity Plan

**Scope**

**The scope of this plan to provide direction to Klamath Falls or Portland Premium Health locations when the BCP is activated by the BCP Program manager.**

**Purpose**

The purpose of a business continuity plan is to provide the organization with the steps needed to continue business operations if normal business operations are disrupted. The intent of this plan is to provide guidance and informed decision making to Premium Health employees and to prepare for any emergency that may occur.

**Assumptions and planning principles-**

* Due to the location of both cities Premium Health operates, the only natural disaster to plan for is an earthquake.
* It is assumed that the AWS servers will never go offline
* It is planned that the maximum amount of time that the organization will operate under the BCP is 24 hours.
* It is also assumed due to the vast amount of resources available in both locations, the maximum amount of time servers will run on generators will be 6 hours.
* The BCP will cover power outage, network outage, earthquake damage, and fire scenarios.
* The priorities in given scenarios will be the data servers and web servers as they’ll be the most sensitive and expensive to replace.

**Incidents to be included**

* power outage
* network outage
* earthquake damage
* Malware spread
* Server outage
* Windows Crash
* A fire to occur

The given scenarios were selected to be part of the BCP as they are the most likely to occur and will need the most planning. Other scenarios may also need in depth planning but don’t have a high chance of occurring or resulting in damage to this given organization.

**System description and architecture**

* Because the server located in the main headquarters will communicate with the server in Klamath falls, it is important to have another ISP in case of an outage. This will allow the organization to run on the BCP until the issue is resolved.
* The workstations are assumed to be shells, meaning user documents and data will be saved on a central server rather then user desktops resulting not being a priority for the BCP.
* At the main headquarters in Portland the database server is critically important as it communicates with the server in Klamath Falls. If the database were to fail offices wouldn’t know anyone’s appointment or patient records.
* The Web server Is also important as it allows users/doctors to communicate sending important medical information.
* The payment server is also important as it has all the payment information for co-pays.
* The remaining servers are critical important as they hold medical information for patients.
* All the servers in the organization are running a standard 2019 windows server with Raid 0.
* Due to HIPPA and patient data on all servers, they are all to be considered private and classified data.

**Responsibilities**

* BCP Program Manager- CEO
* BCP Coordinator- Chief Information Officer
* There will be the following teams for BCP
  + The Technical Recovery Team which will be made of the IT Team
  + Emergency Management Team will be composed of Senior management.
  + Damage Assessment Team will be composed of faculty and HR.

**Notification / activation/Recovery phase**

* Power outage
  + When outage occurs- The BCP coordinator should turn on backup generators. And BCP program manger should stay alert to the cause of earthquake to determine if it is safe to proceed work.
  + 3 hours- If power is not restored and reason of outage is still unknown, with the help of TRT team the organization should relocate power sensitive systems to an alternative location
  + 6 hours- release all personal besides the TRT and stand by to recover systems to original location when power is restored.
* Earthquake
  + When Earthquake hits- The BCP coordinator should message the three groups to meet in a common place to review damage and plan ahead.
  + 1 hour after- Assess any damage, if damage has occurred take appropriate steps to move infrastructure to different location or safely shutdown
  + 3 hours after- Due to the severity of earthquake allow personal to go home or stay alert for aftershocks
* Fire
  + When fire is detected- Depending on the size of the fire, take appropriate action of calling the fire department or using a fire extinguisher to extinguish fire. If fire is too large, wait for fire department.
    - When fire department extinguishes fire- If hardware was damaged, meet with the TRT to get new hardware and backups from the cloud to get running.
  + Once fire is extinguished- Assess damage to any hardware if any. If there is, separate the damaged hardware from the remaining.

**Reconstitution phase**

* If an Earthquake or fire damaged the building extensively, then confidential data would be moved to the Klamath location or another area till restorations for the building are complete. Once building restorations is done the servers would continue run for 3 days at the backup location to ensure there is no service disruptions.
* If an power outage is more then 6 hours, servers would moved to an alternative location where HVAC and proper resources are available to continue operation till power is restored.

**Training, testing, and exercises**

* **BCP training –** Training will occur for all members part of the BCP teams. But also specified training that will go over each member role and job during the BCP implementation.
* **BCP Testing-** The BCP plan will be tested annually to ensure it is up to data and still effective as the organization grows. During the test, each disaster recovery plan will be tested and will reviewed line by line. The testing will also include alternate locations if described in the plans.
* **BCP Test Exercises-** Test situations will occur which a problem will be presented, and the teams will solve them, this will include various method of exercises such as tabletop, functional and full-scale exercises.

**Plan maintenance**

During the testing phase, revisions will be documented and the BCP will be revised at the end of the annual testing. Also if major changes occur to the IT infrastructure such as moving from physical servers to cloud servers, the BCP should be updated as different approaches will be made to save data.

# Disaster Recovery Plan

* Purpose
  + The Disaster Recovery Plan is to ensure Premium Health has a plan to restore critical business processes after a disaster.
* Scope
  + The scope of the DRP will be limited to restoring the critical business process related to the IT infrastructure. This will ensure if any system fails after a disaster it will be brought back to service.
* Disaster / Emergency Declaration
  + The organization will declare an emergency after the CEO communicates with its team that a disaster may strike within 48 hours. When the emergency is declared, the team will meet with their leaders to understand their role in the process. Once the emergency has been declared the team will move to a safe location where the warm site can run the operations.
* Communications
  + All personnel related to Premium Health will be notified via Text message sent out by the emergency system and customers/users that maybe impacted will be communicated via email and a banner on the login page. Across the organization the team leaders will have local copies for their role and their team members, once the text message is sent for the plan to activate, they will know what to do.
* Activities
  + If an emergency were to be declared, staff members would meet with their department leaders to ensure everyone is not injured or missing. Then the servers would be move to an alternative location while the servers in the warm site will launch to take the load while the servers are being relocated. And any important IT infrastructure that cannot be moved such as switches would be shut off to prevent any damage from power outages/spikes.
* Recovery Procedures
  + Server Recovery procedure
    - After a disaster if the server is damaged and a new one is needed, the server will need Windows Server 2019 Installed
    - Once the OS is installed then it will need to restore from a backup in windows using the latest backup downloaded from AWS, this process may take several hours due to the size of the backups
  + Network recovery procedure
    - If the network infrastructure is damaged depending on if it is a switch, router or firewall, it will need to be replaced with the same exact model and upgraded to the same version that the previous networking equipment was running.
    - If networking cabling is damaged, then that will need to be replaced with the same category as the previous cabling.
* Critical Operations
  + Power- There will be backup generators that will operate during/after a disaster, this will help shut down servers, and make it easier for people to move the server to a new site
  + Internet- This will help gather any data and send it to the new location before the physical server gets there, it will also help the organization use their emergency communication system.
  + Firewall- It’s also critical that we keep the organizations defense up even in the case of a disaster, as it may be an attempt for an attacker to steal information.
* Restoration & Normalization
  + Once the disaster has passed, the BCP coordinator will make the call when it is safe to move services back to the original location. Then the least critical functions will be moved and damaged will be assed to see if it is safe to move the most critical functions such as servers.
  + The workstations would be moved first, then the networking infrastructure and then finally the servers.
* Testing
  + DRP testing will occur yearly to ensure the plan is still relevant and will be tested with various methods such as desktop exercises and simulation.
* Maintenance and Updates
  + When the DRP is tested any changes that might occur, or observations will be documented and revised during our yearly testing.

# Computer Incident Response Team Plan

* CIRT Members & Roles
  + Chief Information Officer- Leader of CIRT Teams
  + Klamath Falls Team – Will consist of the IT department and any Security analyst at the location
  + Portland Team- Will consist of the IT department and any Security analyst at the location
* Responsibilities
  + CIO- The CIO will be the team leader for the CIRT teams, this can be in some situations where the CIO is unavailable, then the first to arrive will be the Team Leader. The team leader will also be responsible in developing incident response procedures.
  + Information Security members- These will be composed of the IT members on the team, they will be able to identify source of the breach, recommended solutions and investigate incidents when they occur.
  + Network administrators- Network admins will be composed in the IT team and will be able to recognize abnormal traffic on the network.
  + Physical Security- Security Officers at both locations will know what surveillance is used, the locations and the purpose of these controls.
  + Legal- Premium Health’s attorney will provide any legal remedies when needed against attackers.
  + Human Resources- HR will be involved if the attack originated from a Premium Health employee such as violating AUP.
  + Communications- Public Relations will be part of the team if details of an attack become public, they will help preserve the image of the company.
* Policies
  + Policies need to remind the team what they can and cannot, or should not do, when handling an incident.
  + Here are a couple of examples that are common policies:
    - Do not initiate an attack against someone or something attacking your system. There are many legal implications here, but most importantly, your organization is not equipped to handle a cyberwar.  If you launch an attack, you might be setting yourself up for total cyber attack disaster.
    - Communications with the public are only to be handled by public relations.
    - Public relations shall seek legal counsel with the organization’s lawyer prior to making any formal press releases regarding the organization, its information system, and the data contained within.
  + Incident Handling Process
    - From experience, I prefer to follow NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide. Your textbook recommends the same and does a great job summarizing the publication with an easy to following handling process.  For this assignment, go ahead and include this process, but make sure to cite all of your references.  The process I am referring to is Figure 15-2, Incident response life cycle.
  + Incident Handling Procedures
    - Here, provide a brief overview, chart, and explanation showing the prioritization and incident response for specific critical and non-critical systems. For example, the customer portal that processes payments will probably be a high priority, whereas a kiosk in the customer waiting area is probably low priority.
  + Communication Escalation Procedures
    - Here, be sure to highlight how the team will relay communications up and down the organization. For example, the network administrator should not be going direct to the CEO to brief them on a network security breach.  Instead, maybe the network administrator should escalate the issue to the security team, who escalates to the team member, who can escalate to the CIO.

# citations

Gibson, D. (2015). *Managing Risk in Information Systems ; Second Edition*. Jones and Bartlett Learning.

“Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards.” *PCI Security Standards Council*, [www.pcisecuritystandards.org/](http://www.pcisecuritystandards.org/).

OUHSC Information Technology. (n.d.). Retrieved July 10, 2019, from <https://it.ouhsc.edu/>

J. (Ed.). (2007, October 17). Information Security Risk Management for Healthcare Systems. Retrieved July 10, 2019, from <https://www.medicalimaging.org/wp-content/uploads/2011/02/Information-Security-Risk-Management-for-Healthcare-Systems.pdf>

Wiley\_admin. (2015, February 02). The Purpose of Risk Management in Healthcare. Retrieved July 10, 2019, from https://elearning.scranton.edu/resource/business-leadership/purpose-of-risk-management-in-healthcare