Risk Management Plan

CYBR610 Final Draft

Daniel Carbajal

Bellevue University

June 3, 2023

1. Introduction

This risk management plan defines how our company’s risk management process will be executed. This includes scope, the compliance laws and regulations, the tools and approaches that will be used to perform risk identification, assessment, mitigation and monitoring activities. The risk assessment will start with the methodology which defines the tools and approaches that will be used to perform risk management activities such as risk assessment, risk analysis and risk mitigation strategies A risk register chart will be included, where one can document all the risk identification information of the project. It will provide the risk breakdown structure to identify risk categories and the hierarchical structure of project risks. It will also include a risk assessment matrix to analyze the likelihood and the impact of project risks so that they can be prioritized. Finally, a risk response plan will be provided that explains the risk mitigation strategies that will be employed to manage the project risks.

The plan then includes the key roles and responsibilities of each member of the risk management team. The risk management team members have responsibilities as risk owners. They need to monitor project risks and supervise their risk response actions. Finally, the plan will include the timeline including the proposed schedule of the risk assessment plan. The following sections encompass these and other factors that are required to complete this risk assessment plan.

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project’s objectives (Ct. Gov, 2022). Risk Management is the process of identifying, assessing, responding to, monitoring, and controlling, and reporting risks (Gibson & Igonor, 2022). This Risk Management Plan defines how risks associated with the project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks by the Risk Manager and/or Risk Management Team.

1. Scope and Boundaries of the Plan

The scope of this risk management plan will focus on Health Network and its risk management team and goals set forth to ensure that all criteria for this plan are met. Goals will encompass the ability to create the risk assessment and its mitigation that will allow Health Network secure its health information and its client data from known vulnerabilities and mitigates the risks associated with the storing, receiving, and transmission of data. The scope of the plan includes.

* Identification of all health data
* Storing of health data
* Using health data
* Transmitting health data

The boundaries of this risk management plan will be set within the health data only and not encompass the rest of the IT infrastructure that may not apply to the identified handling of health data by Health Network, and it will ensure that the scope is kept within the confines of securing the health data that is used by Health Network within the scope.

1. Compliance Laws and Regulations

The rules and regulations used in this risk management plan will be as follows:

Health Insurance Portability and Accountability Act – HIPAA

HIPAA ensures that health information data is protected. It has led to improved security and protection of health information and this regulation requires compliance in three areas:

* Administrative – ways to protect patient data and ensure that it can be accessed only by authorized personnel.
* Physical – ways to prevent physical theft and unauthorized access to systems with protected data.
* Technical – using technology to protect computer networks and devices from theft.

All three areas will be covered and within the scope of the plan to protect Health Network’s health data and information systems. The HIPAA compliance calls for the continuous cycle of the following steps which will encompass the scope and information requirements for this plan as follows:

* Assessment
* Risk Analysis
* Plan Creation
* Plan Implementation
* Continuous Monitoring

Health Network will use this risk assessment plan to meet compliance with HIPPA and all its requirements.

1. Qualitative Risk Assessment

Risk assessments address the potential impacts to organization’s operations and assets arising from the operation and use of information systems and the information processed, stored, and transmitted by those systems (NIST, 2021). Organizations conduct risk assessments to determine risks that are common to the organization’s core missions, business functions, as well as common infrastructure and support services. Risk assessments can support a wide variety of risk-based decisions and activities by organizational officials, and they will be used by Health Network and its three main products to ensure they meet compliance and keep client and patient data secure. This risk assessment plan will be used to investigate, detect and mitigate risks within Health Network and its information security infrastructure.

Risk is a measure of the extent to which an entity is threatened by a potential event, and is typically a function of: the adverse impacts that would arise if the event occurs; and the likelihood of occurrence (NIST, 2021). Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information and reflect the potential adverse impacts to organizational operations. Risk assessment is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the careful analysis of threat and vulnerability information for Health Network, to determine the extent to which these events could adversely impact the organization and the likelihood that such circumstances or events will occur.

Scope and Boundaries of Risk Assessment Plan

The scope of this risk assessment plan will focus on Health Network and its risk management team and goals set forth by the overall Risk Management Plan. Goals will encompass the ability to create the risk assessment and its mitigation that will allow Health Network secure its health information and its client data from the following three main areas:

* HNetExchange is the primary source of revenue for the company. This service handles secure electronic medical messages that originate from its customers, such as large hospitals, which are then routed to receiving customers such as clinics.
* HNetPay is a web portal used by many of the company’s HNetExchange customers to support the management of secure payments and billing. The HNetPay web portal, hosted at Health Network production sites, accepts various forms of payments and interacts with credit-card processing organizations.
* HNetConnect is an online directory that lists doctors, clinics, and other medical facilities to allow Health Network customers to find the right type of care at the right locations. It contains doctors’ personal information, work addresses, medical certifications, and types of services that the doctors and clinics offer. Doctors are given credentials and can update the information in their profile.

The threats identified and the risk assessment are included in Table 1 attached to this document. Titled Health Network Assessment. The types of controls to be assessed will encompass the mitigation of the risks based on the risk assessment. They will include the following.

* Backup power for cases of loss of power due to local power outages and national disasters
* Firewall and double password authentication to access all customer data as well as customer login.
* Computer and software penetration tests and security assessments
* Encryption of transmitted and sent data.
* Intrusion detection systems
* Badge and Physical security mechanisms to each of Health Networks
* Third Party 24/7 monitoring of hardware and network systems.
* Internal accounting controls
* Operational controls to include processing documents and client data
* Administrative controls to include password management and personnel logging information.
* Organizational security policies and procedures to be reviewed and monitored frequently.
* Procedures and practices to ensure adequate safeguards over access.
* Physical and logical security policies for all data centers and IT resources

1. Risk Mitigation Plan

This risk mitigation plan encompasses the risks found during the risk assessment and

described in the form called Health Network Risk Mitigation Plan. The overall risk mitigation uses certain methods of control as countermeasures in order to provide the best possible security of Health Network data and client information. Several policies will be implemented to let users know what they can and cannot do with the systems. Technical controls were used to apply actual software and hardware related countermeasures to secure the network infrastructure. And finally, some physical controls will be implemented to secure the network infrastructure and the facilities from theft, natural disasters, or other damage by fire, flooding, or physical removal or theft of a system within Health Network’s premises.

The first set of countermeasures applied to Health Network include generating policies and procedures that will control the way a user accesses and uses system accounts and information. For example, in order to ensure safety some privacy will be removed from the user’s as any employee or user accessing a device or network within Health Network will be subject to scanning of emails and network traffic. Some restrictions will be applied to the use of certain sites to include sexual or pornographic content for the security of all people and to prevent possible malicious attacks that can stem from these sites. Some streaming sites such as Netflix and Pandora will be restricted to prevent the network from being overloaded with unnecessary network traffic.

There will also be policies on how to login and logout out a Health Network device to ensure that everyone follows the same basic principles of network and data use. A strong password usage policy will be employed in order to allow users to not write down logins and passwords and to generate strong passwords to ensure login information is secure. The limitation of login attempts with will also be employed to ensure the user will have to ask for a new password before being able to login into the system again. Users will also be required to lock their accounts and screens whenever they leave their desks or step away from devices using Health Network information. Emails are to be kept professionally and the use of personal email addresses for forwarding Health Network information is also prohibited. These restrictions will be enforced and not following these instructions could lead to reprimand or up to employee termination.

Physical controls will be the next step of risk mitigation and will provide the software and hardware from which the policies and procedures can be implemented and enforced. The use of firewalls, secure routers, and intrusion detection systems will be employed in order to protect the network infrastructure. One thing that will be used in conjunction with policy will be a password generation tool to encourage strong passwords and to prevent a user from trying to login with the wrong password more than three consecutive attempts. This will protect HNetPay and HNetExchange accounts from being tampered with or easily defeated using a password dictionary or brute force attack. System logs and audit trails will also be implemented to log all important information and be able to detect and retrace steps from a possible attack. This will provide the who, what, where, and when of security events as they occur on a system. Events will be logged as deemed necessary for example logins or attempted access to HealthNet and other client information will be logged to ensure that only authorized personnel are accessing these services.

Firewalls and Routers will be configured to allow only private network traffic and all other information will flow in and out of the network through a firewall and proxy server. This will ensure that all access within the network will be limited to HealthNet employees, and ports from which to access this data will be assigned and all other ports will be closed or restricted in use. Encryption and VPN will be used to access payments and accounts receivable as well as doctors and other services as they are added into the list for Health Network. A public key system will be established for any other access or transfer of data from an outside network. This will allow Health Network to protect and provide security to all its workings and system information.

Finally, physical controls will be provided as countermeasures based on potential natural disasters or physical theft or unauthorized access. The use of badges will be required to enter the building and along with a not ‘piggy backing’ policy will ensure all employees and visitors are properly badged and can only enter the building if they have the proper identification and authorization. A separate lock and 24/7 camera monitoring system will be placed at the entrance of the data servers to ensure that these systems are secure and no unauthorized personnel can easily access them. Fire detection and suppression will be implemented and to secure the data servers as well as the infrastructure and employees within the building. Finally, locks will be placed in all doors of the building to ensure that information is confined to the premises and only authorized personnel are allowed to enter the premises.

It will be important to ensure these counter measures protect the information for Health Network. Policies and procedures along with technical and physical controls will be implemented as countermeasures to ensure data is kept safe and secure. One must ensure that the countermeasures will comply with HIPAA and PCI DSS standards and regulations. The cost of not complying can be high so these countermeasures will be implemented in this risk mitigation plan in order to ensure compliance and proper security of Health Network’s information and infrastructure.

1. **Business Impact Analysis (BIA)**

***1. Overview***

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the Health Network, Inc. (Health Network*).* It was prepared on May 21, 2023

***1.1 Purpose***

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports and using this information to characterize the impact on the process(es) if the system were unavailable.

The BIA is composed of the following three steps:

1. **Determine mission/business processes and recovery criticality.** Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible.  Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

This document is used to build the *Health Network* Information System Contingency Plan (ISCP) and is included as a key component of the ISCP. It also may be used to support the development of other contingency plans associated with the system, including, but not limited to, the Disaster Recovery Plan (DRP) or Cyber Incident Response Plan.

***2. System Description***

Health Network has three main products: HNetExchange, HNetPay, and HNetConnect.

* HNetExchange is the primary source of revenue for the company. This service handles secure electronic medical messages that originate from its customers, such as large hospitals, which are then routed to receiving customers such as clinics.
* HNetPay is a web portal used by many of the company’s HNetExchange customers to support the management of secure payments and billing. The HNetPay web portal, hosted at Health Network production sites, accepts various forms of payments and interacts with credit-card processing organizations.
* HNetConnect is an online directory that lists doctors, clinics, and other medical facilities to allow Health Network customers to find the right type of care at the right locations. It contains doctors’ personal information, work addresses, medical certifications, and types of services that the doctors and clinics offer. Doctors are given credentials and can update the information in their profile.

Health Network customers, which are the hospitals and clinics, connect to all three of the company’s products using HTTPS connections. Doctors and potential patients can make payments and update their profiles using Internet-accessible HTTPS websites.

Information Technology Infrastructure Overview

Health Network operates in three production data centers that provide high availability across the company’s products. The data centers host about 1,000 production servers, and Health Network maintains 650 corporate laptops and company-issued mobile devices for its employees.

***3. BIA Data Collection***

Data collection will be accomplished through individual/group interviews email and questionnaire with the goal to have all stakeholders have an input into the data collection process.

***3.1 Determine Process and System Criticality***

**Step one of the BIA process** - Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), identify the specific mission/business processes that depend on or support the information system.

| **Mission/Business Process** | **Description** |
| --- | --- |
| *Send Secure Electronic Medical Messages* | *Process handles secure electronic medical messages that originate from its customers* |
| Allow for *Client Payment* | *Process of taking electronic payments from clients and storing data and sending invoice back to clients* |
| *Send and Review Client Billing* | *Process of issuing billing to clients and keeping information stored and accessible to HealthNet employees and its clients* |
| *Access and Store on Online Directory* | *Store doctors’ personal information, work addresses, medical certifications, and types of services that the doctors and clinics offer* |
| *Sustain HTTPS Connections* | *Process for doctors and potential patients use to make payments and update their profiles* |
| *Access to HTTPS Websites* | *Process of providing internet accessible websites to clients and patients to make appointments and handle billing* |

***3.1.1 Identify Outage Impacts and Estimated Downtime***

*This section identifies and characterizes the types of impact categories that a system disruption is likely to create in addition to those identified by the FIPS 199 impact level, as well as the estimated downtime that the organization can tolerate for a given process*

***Outage Impacts***

*.*

The following impact categories represent important areas for consideration in the event of a disruption or impact.

Impact values for assessing category impact:

* Severe = Loss of Revenue
* Moderate = Higher time to achieve
* Minimal = Low loss of revenue

The table below summarizes the impact on each mission/business process if *HealthNetwork* were unavailable, based on the following criteria:

| **Mission/Business Process** | **Impact Category** | | | | |
| --- | --- | --- | --- | --- | --- |
| **Cost** | **Loss of Data** | **Hardware Loss** | **Loss of Client** | **Impact** |
| *Send Secure Electronic Medical Messages* | *Severe* | *Severe* | *Moderate* | *Moderate* | *Severe* |
| Allow for *Client Payment* | Moderate | Severe | Moderate | Severe | Moderate |
| *Send and Review Client Billing* | Moderate | Severe | Moderate | Severe | Moderate |
| *Access and Store on Online Directory* | Severe | Severe | Severe | Moderate | Severe |
| *Sustain HTTPS Connections* | Severe | Severe | Severe | Severe | Severe |
| *Access to HTTPS Websites* | Moderate | Severe | Severe | Severe | Severe |

***Estimated Downtime***

Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the downtime factors for consideration as a result of a disruptive event.

* **Maximum Tolerable Downtime (MAO).**  The MAO represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MAO is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.
* **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MAO. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MAO.
* **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

The table below identifies the MAO, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on Health Network.

| **Mission/Business Process** | **MAO** | **RTO** | **RPO** |
| --- | --- | --- | --- |
| *Send Secure Electronic Medical Messages* | *12 hours* | *4 hours* | *8 hours (last backup)* |
| Allow for *Client Payment* | *72 hours* | *24 hours* | *24 hours (none)* |
| *Send and Review Client Billing* | *72 hours* | *24 hours* | *24 hours (last backup)* |
| *Access and Store on Online Directory* | *24 hours* | *12 hours* | *8 hours (last backup)* |
| *Sustain HTTPS Connections* | *12 hours* | *4 hours* | *4 hours (none)* |
| *Access to HTTPS Websites* | *24 hours* | *12 hours* | *8 hours (none)* |

***2 Identify Resource Requirements***

The following table identifies the resources for the mission/business processes that compose Health Network including hardware, software, and other resources such as data files.

|  |  |  |
| --- | --- | --- |
| **System Resource/Component** | **Platform/OS/Version (as applicable)** | Description |
| ***HTTPS Web Servers*** | ***Optiplex GX280*** | ***Web Site Hosts*** |
| ***Payment Application*** | ***Visa Payment App*** | ***Credit Card Processor Application*** |
| ***Online Database Servers*** | ***Oracle Dell Servers*** | ***Database servers*** |
| ***Corporate Laptops*** | ***HP Envy 7256*** | ***Personal Laptop*** |
| ***Employee Devices*** | ***Dell Inspiron i7 -7002*** | ***Personal Laptop*** |
| ***Billing Application*** | ***QuickBooks Professional*** | ***Billing Web Invoices*** |
| ***Firewall*** | ***SonicWall TZ 400*** | ***Internet Firewall*** |
| ***Internet Routers*** | ***ISR 4331*** | ***Internet Routers for Network Access*** |
| ***Air Conditioning*** | ***Daikin 5 Ton 13*** | ***Air Conditioning for Servers*** |
| ***Power Generator*** | ***Generac Guardian*** | ***Power Outage Backup Generator*** |

***3.3 Identify Recovery Priorities for System Resources***

The table below lists the order of recovery for Health Network resources. The table also identifies the expected time for recovering the resource following a “worst case” (complete rebuild/repair or replacement) disruption.

* **Recovery Time Objective (RTO)** - RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

| **Priority** | **System Resource/Component** | **Recovery Time Objective** |
| --- | --- | --- |
| ***HTTPS Web Servers*** | ***Optiplex GX280*** | ***8 hours to rebuild or replace / (backup servers in place)*** |
| ***Payment Application*** | ***Visa Payment App*** | ***72 hours to get back online or replace*** |
| ***Online Database Servers*** | ***Oracle Dell Servers*** | ***24 hours to rebuild or replace / (backup servers in place)*** |
| ***Corporate Laptops*** | ***HP Envy 7256*** | ***48 hours to rebuild or replace*** |
| ***Employee Devices*** | ***Dell Inspiron i7 -7002*** | ***72 hours to rebuild or replace*** |
| ***Billing Application*** | ***QuickBooks Professional*** | ***72 hours to get back online or replace*** |
| ***Firewall*** | ***SonicWall TZ 400*** | ***24 hrs to get back online or replace (redundant firewall access point available)*** |
| ***Internet Routers*** | ***ISR 4331*** | ***24 hrs to get back online or replace (redundant internet routers available)*** |
| ***Air Conditioning*** | ***Daikin 5 Ton 13*** | ***4 hours to rebuild or replace*** |
| ***Power Generator*** | ***Generac Guardian*** | ***72 hours to rebuild or replace*** |

1. **Business Continuity Plan (BCP)**

This business continuity plan (BCP) is established to provide a plan to recover Health Networks assets based on the priorities and CBFs that are required to get all client server systems up and running once again. This plan lists the steps to recover the necessary business functions in case of a disruption including the possibility of a major snowstorm which is common in the corporate location. The following is the steps need to recover Health Network’s data servers and web applications for customers with the least amount of impact on the organization’s major operations.

***Business Function Recovery Priorities***

In case of a disruption and need for recovery, the following priorities will be set. The priority will be to see which site or location has been impacted and see what data may have been there that needs to be at the other two sites. The BCP team will establish back-up procedures for all essential tasks and training will be provided so essential personnel can perform the tasks. The team will ensure customer transactions can still be processed, even if systems failures delay the transactions. This will ensure HNetExchange, HNetPay, and HNetConnect. are all available to clients and employees within the MAO established by the BIA. The other priority will be to develop a systems failover for networks and servers. The team will also test back-up procedures frequently and measure testing outcomes to ensure that any changes that need to be made can be done before a disruption occurs and the BCP needs to be carried out.

***Relocation Site Strategy***

The relocation site strategy will be done to help safeguard sever and corporate offices for relocation against the unexpected:

* The IT team will inventory all software and hardware, servers, storage and networking equipment that needs to be relocated.
* The IT team will ensure that the other stie locations are ready and running to take on the lost server payload site.
* Backup copies of important data including firewalls & servers will be made and sent over to the other three locations.
* The team will arrange for copies of the backup to be stored at one of the two other server data centers where it will be ready for relocation.
* The team will have to switch phone lines, numbers, internet connections, migration of data and transfer of servers for Health Network data.
* There will be a list all your business priorities and data classified according to Critical Business Functions
* An emergency contact list to include IT & Vendor Technicians as well as all internal IT team members needed for the relocation.

***Recovery Plan***

The recovery plan will consist of the following steps to ensure Health Network is prepared to recover once a disruption or incident has occurred.

Identify Potential Threats – Health Networks geographical locations are more vulnerable to certain types of disasters than others. We need to consider the high probability of certain events occurring, including power outages, extreme cold and events that could make your employees' commutes impossible or dangerous. Must be prepared to have relocated site running and have employees work from home if possible.

Collect and Store Information - Health Network needs to collect information for essential business, employees, and vendors. Access to this information is critical after a disaster or emergency. The plan will ensure the other sites have the needed stored information to keep business functioning as usual as possible.

Business information - Health Network should have its business licenses and registrations, and its organizational documents. A copy of its professional licenses, leases or property deeds, banking account information and software licenses should be stored in a place where corporate can reach them in case the corporate office is one of the sites that is impacted by an event.

Vendors and suppliers – Health Network should store important account numbers and account information for all suppliers and vendors, and anything needed to keep the data centers running in case one or more of the sites is involved in a disaster or impactful event.

Employee data - Gather employee names, addresses, phone numbers and emergency contact information.

Emergency Equipment -. Emergency generators and backup power supplies can provide Health Network the power you need to continue operating your business in case of a power outage. If the site needs to be relocated, emergency will allow Health Network to shut down operations securely and safely.

***Recovery Procedures***

The following Recovery Procedure will be used in case of disaster or incident occurring

* Disaster Incident Occurs
* Notification of Management
* Preliminary Damage Assessment
* Declaration of Disaster
* Plan Activation
* Relocation to Alternate Site(s)
* Implementation of Recovery Plan Procedure
* Establishment of Communication
* Restoration of Data Process and Communication with Backup Sites
* Commencement of Alternate Site Operations
* Management of Work
* Reconstitution Phase
* Cessation of Alternate Site Procedures
* Relocation of Resources Back to Primary Site

***Reconstitution Plan***

After the phase the organization will begin the process to relocate the resources back to the primary site.

* Ensure damage at site locations is repaired.
* Talk to insurance and have new site ready if old site is too damaged to repair.
* Ensure the safety of employees and personnel is verified.
* Have data centers and IT systems back and running.
* Have concurrent sites operational.
* Move personnel back to normal location.
* Deactivate plan and return to normal procedures.

***Testing and Training Plan***

Training will be provided to all personnel to ensure that BCP is viable and implementable. There will be a training session for all teams to get everyone on board with the plan and to see how each person fits into the success of the plan. There will be testing of individual steps within the BCP so that everyone is aware of how to work and to verify and change anything that is necessary to make plan a success. Test will be run to test on alternate locations and resources and especially as to how corporate and its offices will run in case of a relocation or work stoppage is required. This will be done with an effort to not impact normal functions or operations of Health Network.

There will be some BCP test exercises in the form of tabletop exercises where all members of the team are brought together in the conference room (Igonor & Gibson, 2022). There will also be some functional exercises to ensure that the functionality of the data centers and web applications is feasible while changing operations from one data center to the other.

***BCP Conclusion***

This will be the BCP enacted in case of a disaster to ensure operations within Health Network can meet the MAO requirements and business can function ‘as usual’ within the allotted times responses. The plan will be frequently reviewed and training will be conducted to keep everyone on page and to ensure that any changes to the plan are done periodically and it is kept up to date.

1. **Key Responsibilities**

The roles and responsibilities of this business plan are encompassed in the table below. Each member of the risk management plan team will hold a key role in ensuring the plan is well executed and the scope of the risk management plan is met and completed in accordance with the guidelines of this plan and the laws and regulations concerning Health Network and its compliance with the security of its health data and pertinent information.

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Health Networks SME (HNSME) | The HNSME assists in identifying and determining the context, consequence, impact, timing, and priority of the risk. |
| Risk Manager | The Risk Manager or PM is a member of the Integrated Project Team (IPT). The Risk Manager determines if the Risk is unique, identifies risk interdependencies across projects, verifies if risk is internal or external to project, assigns risk classification and tracking number. During the life of the project, they continually monitor the projects for potential risks. |
| Integrated Project Team | The IPT is responsible for identifying the risks, the dependencies of the risk within the project, the context and consequence of the risk. They are also responsible for determining the impact, timing, and priority of the risk as well as formulating the risk statements. |
| Risk Owner(s) | The risk owner determines which risks require mitigation and contingency plans, he/she generates the risk mitigation and contingency strategies and performs a cost benefit analysis of the proposed strategies. The risk owner is responsible for monitoring and controlling and updating the status of the risk throughout the project lifecycle. The risk owner can be a member of the project team. |
| Other Key Stakeholders | The other stakeholders assist in identifying and determining the context, consequence, impact, timing, and priority of the risk. |

The responsibilities of Health Network and meeting HIPAA compliance will include:

* A list of all health information sources.
* Inspection results for all data sources regarding their compliance with HIPAA.
* How the data is stored.
* How the data is protected.
* How the data is transmitted.
* A list of existing HIPAA policies used by Health Networks.
* A list of needed HIPAA policies used.
* A list of recommended solutions to ensure compliance with HIPAA.
* Costs for each of the recommended solutions.
* Costs associated with noncompliance with HIPAA.

The IT department is expected to provide the following:

* Identification of access controls used for data.
* A list of recommended solutions to ensure compliance with HIPAA.
* Cost for each of the recommended solutions.

A CFO will validate the data provided by the IT and sales departments and complete a cost benefit analysis (CBA).

1. **Proposed Schedule**

The schedule includes the following:

* Compliance laws and regulations assessment 4/11/2023
* Risk assessment tools research. 4/15/2023
* Risk identification 4/17/2023
* Risk assessment, 4/23/2023
* Risk mitigation 4/30/2023
* Business Impact Analysis 5/20/2023
* Business Continuity Plan 5/21/2023
* Risk monitoring activities 5/30/2023

1. **Continuous Monitoring**

NIST SP 800-137 defines continuous monitoring (CM) as ongoing. awareness of information security, vulnerabilities, and threats. to facilitate risk-based decision making (NIST, 2021).

•CM will be embedded in a comprehensive information security program, following NIST RMF

•NIST RMF relies on continuous monitoring to provide ongoing assessment and authorization of systems

•CM will require assessment of all security controls, including management and operational controls that cannot be assessed using automated tools

•CM requires both automated and manual processes

•Where possible, automated tools can improve CM efficiency and cost-effectiveness

•NIST SP 800-53 technical controls can be monitored with automated tools

1. **Conclusion**

Risk management is an important process that managers should maintain in an organization. It is inevitable to take risks and managers should have better strategies to deal with risks. The long-term survival of an organization depends on the ability to manage risks. This risk management plan assesses some of the risks and ensures that a path is set to protect Health Networks assets. This plan includes the processes, policies and procedures, and the steps necessary to ensure that Health Networks infrastructure and the organization as a whole will be protected in the future and a plan is devised to continually update, test, and ensure that risk is mitigated as much as possible for the foreseeable future.

. **References**

Ct Government Portal, Risk Management Plan, 2022, <https://portal.ct.gov/-/media/Departments-and-Agencies/DSS/CT-METS/Library/General/CTDSSRiskManagementPlanv11.pdf?la=en&hash=6DBD5DB2BD78DCB8559845A2FB343AF1>

Gibson, D., Igonor, A., Managing Risk in Information Systems, Third Edition, Jones & Barttlet Learning, 2022.

NIST 800-30r1, December 2021, Risk Assessment Framework,

YouTubeVideo: Business Impact Analysis (12:50 minutes), James Myers, August 2011

BCP Template from BCP Plan website

<https://legaltemplates.net/form/lt/business-continuity-plan/?utm_source=google&utm_medium=cpc&utm_campaign=129-Business%20Continuity%20Plan&utm_term=business%20continuity%20plan%20template&utm_campaign_id=16962902305&utm_adgroup=Business%20Continuity%20Plan&utm_adgroup_id=135330133426&utm_content=593760358931&gclid=CjwKCAjw3ueiBhBmEiwA4BhspFhNWgZ4krZZjzhnAeF2kG7If0PC8uko5eKqCmncrtqXK1w5RvGYRxoCtA4QAvD_BwE>

Vaida, D., April 2022 Business Continuity Planning, Wall Street Mojo, <https://www.wallstreetmojo.com/business-continuity-planning/>