Risk Management Plan 2025 for:

HEALTH NETWORK INC.

Thomas Juricek

Health Network Inc. – IT Security Intern

Table of Contents

Part 1 – Risk Management Plan Outline and Research

1. Introduction

In healthcare, risk management is not only the best practice for protecting patients and ensuring operational continuity, but also a legal and regulatory requirement. By developing a risk management plan, the organization reduces the likelihood of security incidents, enhances patient and stakeholder trust, and demonstrates compliance with applicable laws and industry standards. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) establish the legal requirements for protecting Protected Health Information (PHI), while industry standards like the HITRUST Common Security Framework (CSF) provide a unified approach to achieving compliance with HIPAA, NIST, ISO, and PCI DSS. These frameworks set expectations for how healthcare organizations must manage information security and risk, ensuring both regulatory compliance and industry best practices.

2. Purpose and Importance

The Purpose of the risk management plan is to provide a roadmap for managing risks that could affect the confidentiality, integrity, and availability of critical healthcare systems and data. It establishes clear processes for identifying potential threats, evaluating the likelihood and impact of those threats, and implementing safeguards to minimize exposure. The plan ensures that organizations can meet operational objectives while protecting patients, staff, and stakeholders from unnecessary harm. Breaches or system failures can result not only in financial penalties and legal consequences but also in diminished confidence in the organization's ability to deliver quality care. By implementing a structured and ongoing risk management program, the organization strengthens its defenses against these outcomes while demonstrating accountability and

responsibility. In addition, this plan helps align the organization with industry recognized frameworks such as HIPAA and HITRUST, and broader standards like the NIST Cybersecurity Framework and ISO/IEC 27001. Adhering to these frameworks highlights the organization's commitment to excellence, establishes a competitive advantage, and ensures that risk management is taken seriously.

3. Scope and Boundaries

The scope of this risk management plan encompasses all information, systems, processes, personnel, and facilities that support the delivery of healthcare services within Health Network Inc. This includes electronic health record (EHR) systems, network infrastructure, cloud-based services, medical devices connected to the network, and all systems that store, process, or transmit Protected Health Information (PHI). The plan also applies to the organization's physical locations, including hospitals, clinics, and administrative offices, as well as any remote or telehealth services provided. The boundaries of this plan are defined by the systems and operations that are under the organization's control. Third party vendors, contractors, and business associates who handle PHI on behalf of the organization fall within scope to the extent required by HIPAA and Business Associate Agreements (BAAs). However, risks tied to external entities outside the organization's control, such as the broader internet or public infrastructure, are not directly managed within this plan but are considered in terms of their potential impact on organizational operations.

4. Compliance Laws and Regulations

a. Compliance Laws

PCI DSS (Payment Card Industry Data Security Standard)

- An industry-mandated standard that establishes technical and operational requirements for protecting cardholder data during processing, storage, and transmission. Compliance is required for any organization that accepts credit or debit card payments. The standard is organized into 12 primary requirements, shown in the table below:

PCI DSS REQUIREMENTS			
1.	Install and maintain network security controls	**7.**	Restrict access to cardholder data by business need-to-know.
2.	Do not use vendor-supplied defaults for system passwords	**8.**	Identify and authenticate access to system components.
3.	Protect stored cardholder data.	**9.**	Restrict physical access to cardholder data.
4.	Encrypt transmission of cardholder data across open, public networks.	**10.**	Track and monitor all access to network resources and cardholder data.
5.	Protect all systems against malware and regularly update anti-virus software.	**11.**	Regularly test security systems and processes.
6.	Develop and maintain secure systems and applications.	**12.**	Maintain a policy that addresses information security for all personnel.

- Since Health Network Inc. will be processing patient payments via card, adherence to PCI DSS ensures secure financial transactions, reduces the risk of fraud, and demonstrates accountability to both patients and payment processors.

b. Regulations

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA is a U.S. federal law that establishes national standards for protecting Protected Health Information (PHI). It requires healthcare organizations and their business associates to implement safeguards that ensure the confidentiality, integrity, and availability of PHI. HIPAA forms the foundation of modern healthcare compliance.

HIPAA Privacy Rule

- The Privacy Rule defines how PHI may be used and disclosed, setting limits on access and establishing patients' rights to control their personal information.

HIPAA Security Rule

- The Security Rule requires administrative, physical, and technical safeguards to protect PHI that is created, stored, or transmitted electronically. It ensures organizations maintain proper security controls aligned with the sensitivity of healthcare data.

Information Technology for Economic and Clinical Health (HITECH) Act

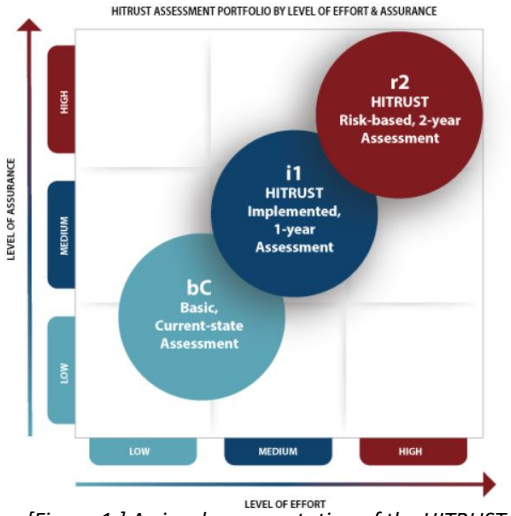
- The HITECH Act builds on HIPAA by strengthening enforcement measures and encouraging the adoption of electronic health records (EHRs). It also introduced requirements such as breach notification, ensuring that patients and regulators are informed promptly in the event of a PHI compromise.

Breach Notification Rule (HITECH)

- As part of the HITECH Act, this regulation mandates that covered entities notify affected individuals, the Department of Health and Human Services (HHS), and in some cases the media, if a data breach involving PHI occurs.

HITRUST CSF (Common Security Framework)

HITRUST CSF is an industry standard, that combines multiple compliance requirements (HIPAA, HITECH, PCI DSS, NIST, ISO/IEC 27001) into a single program. While not a law or regulation, it is widely recognized across the healthcare industry as a benchmark for strong security and compliance practices. Achieving HITRUST certification is a strategic priority, as it demonstrates alignment with HIPAA and other regulatory requirements while providing assurance to patients, partners, and insurers. Health Network Inc. best fits the HITRUST i1 certification, as it offers the best balance of financial costs, administrative workload, and security assurance (Fig. 1). Given the organization's size, the i1 assessment provides an appropriate level of rigor while still meeting partner and regulatory expectations.



[Figure 1.] A visual representation of the HITRUST certification tiers.

5. Roles and Responsibilities

To effectively manage risk, clear roles and responsibilities must be assigned throughout the organization. At Health Network Inc., risk management is a shared responsibility, with leadership setting direction and oversight, and all employees contributing to the protection of sensitive data and systems.

- **Executive Leadership**
    - Provide strategic oversight of risk management initiatives.
    - Approve the risk management plan and allocate necessary resources.
    - Ensure organizational compliance with federal and state laws (HIPAA, HITECH) and industry frameworks (HITRUST, PCI DSS).
- **Chief Executive Officer (CEO)**
    - Holds ultimate accountability for risk management within the organization.
    - Ensures risk management objectives align with business goals and patient care priorities.
    - Serves as the executive sponsor for compliance certifications
- **Chief Information Officer (CIO)**
    - Oversee IT operations and ensure systems support organizational objectives.
    - Coordinates with the CISO to align IT practices with security and compliance requirements.
    - Ensures that new technologies and vendors are evaluated for risk prior to adoption.
- **Compliance Officer**
    - Ensures compliance with HIPAA, HITECH, and other healthcare specific regulations.
    - Manages privacy practices, including PHI use and disclosure monitoring.
    - Coordinates audits, documentation, and regulatory reporting.
    - Oversees auditing of medical record access logs to detect inappropriate or unauthorized use.

- **Department Managers (Clinical, Financial, etc.)**
    - Ensure staff within their departments follow established security policies and procedures.
    - Identify department-specific risks and report them to leadership.
- **IT and Security Staff**
    - Implement, monitor, and maintain technical controls.
    - Conduct system patching, vulnerability management, and incident response.

6. Project Schedule

The risk management plan will be completed in four parts according to the project timeline. Each part builds on the previous deliverables to ensure a structured and comprehensive final plan. The schedule is as follows:

Part #	Description	Due Date
1.	Draft of the introduction, scope and boundaries, compliance laws/regulations, and roles/responsibilities	9/28
2.	Draft of Risk Assessment Plan, including risk identification, identified threats and vulnerabilities, Qualitative Risk Analysis, Response planning, and controls.	10/19
3.	Risk mitigation plan, including known threats, new threats, controls to mitigate, and possible future threats to the organization	11/9
4.	Business Impact Analysis (BIA) & Business Continuity Plan (BCP), including estimated impacts and downtime.	11/23
5.	**Final draft of the Risk Management Plan**	12/11

Part 2 – Risk Assessment Plan

1. Purpose and Importance

The purpose of this risk assessment plan is to identify and evaluate the potential threats and vulnerabilities that could impact Health Network Inc.'s operations and data security. By understanding these risks, the organization can prioritize what needs to be addressed first and take proactive steps to minimize the chances of disruptions or breaches. This assessment helps ensure that patient information stays protected and that healthcare services can continue running smoothly, even when issues arise.

The importance of this plan is that it gives leadership and staff a clear view of where the organization might be vulnerable. Instead of reacting to problems after they happen, this plan supports a proactive approach, anticipating issues, planning responses, and maintaining compliance with regulations like HIPAA and HITRUST. Overall, it keeps the organization more prepared, secure, and confident in its ability to manage risk effectively.

2. Scope and Boundaries

The scope of this risk assessment plan covers all systems, data, and operations that support Health Network Inc.'s daily activities. This includes the data center, electronic health records (EHR) systems, network devices, servers, and any connected medical equipment or cloud services. It also applies to employees, contractors, and vendors who handle or access sensitive information. The goal is to make sure every part of the organization that could be affected by a risk is properly reviewed and protected.

The boundaries of this plan focus on the systems and environments under Health Network Inc.'s direct control. Risks tied to third-party providers or external networks are considered, but only to the extent that they can impact the organization's own operations. This means while outside threats are acknowledged, the plan mainly focuses on what the organization can actively manage and secure.

3. Data Center Assets and Activities

Health Network Inc.'s assets that need to be assessed include all critical components that support IT operations and the delivery of healthcare services. These assets include physical and virtual servers, network switches, routers, firewalls, storage devices, and backup systems housed within the data center. The assessment also covers software applications such as the electronic health record (EHR) system, billing and scheduling platforms, patient communication tools, and other systems that store or process Protected Health Information (PHI). Additionally, environmental and physical security controls, like power supply, HVAC, and access control systems, are key assets that must be evaluated to ensure reliability and compliance.

The activities that need to be assessed involve day-to-day operations that keep these systems functional and secure. This includes data storage and processing, system monitoring, patching and updates, backup and recovery, user access management, and network performance monitoring. Security related activities, such as vulnerability scanning, log review, and incident response, are also critical to evaluate. These assessments help ensure that Health Network Inc. maintains confidentiality, integrity, and availability of its systems while minimizing the impact of potential risks on patient care and organizational operations.

4. Risk Identification

Risk identification for Health Network Inc. will involve collaboration between the project team, IT security staff, department managers, and executive leadership to identify potential threats and vulnerabilities that could impact operations or patient data. This process will evaluate both internal and external factors such as system reliability, user behavior, environmental conditions, and vendor dependencies. The team will also assess how organizational culture, staff levels, and change management practices may contribute to risk exposure.

During this process, the project team will review key documents, including the project scope, schedule, cost estimates, and quality objectives, to identify areas where risks may arise. Careful attention will be given to project deliverables, assumptions, and constraints to pinpoint potential weak points. Risks could include system outages, hardware or software failures, unauthorized access to Protected Health Information (PHI), power disruptions, or delays caused by third party vendors.

By identifying these risks early, Health Network Inc. can prioritize mitigation efforts and allocate resources effectively. This ensures that any technical, operational, or compliance related risks are managed before they impact patient care, system availability, or regulatory compliance.

a. Methods for Risk Identification

Health Network Inc. will use a combination of collaborative discussions, data analysis, and documentation reviews to identify potential risks. These methods help ensure that both technical and non-technical risks are considered throughout the assessment process.

1. Brainstorming

Team members and stakeholders will meet to discuss possible risks based on experience, prior incidents, and knowledge of the organization's systems and workflows.

2. Interviews and Surveys

Department managers, IT staff, and clinical users will be interviewed or surveyed to identify operational challenges, potential security gaps, or recurring issues.

3. SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats)

This structured review helps identify internal weaknesses and external threats that could impact the organization's security posture or operations.

4. Historical Review

Past security events, audit findings, and incident reports will be analyzed to uncover patterns or recurring vulnerabilities that could pose future risks.4

5. System and Network Diagram Review

Reviewing architecture diagrams and network maps helps identify single points of failure, misconfigurations, or outdated technologies.

6. Compliance and Policy Review

Evaluating existing policies and regulations such as HIPAA, HITECH, and internal procedures helps identify compliance related risks.

7. Automated Tools and Scans

Security tools such as vulnerability scanners, log analyzers, and configuration audits will be used to detect technical risks that might not be visible through manual review.

5. Identified Threats and Vulnerabilities

Identified Threat/Vulnerability	Overview of Threat/Vulnerability
Phishing/Malware	Attackers trick staff into clicking harmful links or files that compromise systems or data.
Unauthorized Access to PHI	Someone gains access to patient information without proper permissions.
System or Network Failure	Critical systems stop working due to hardware, software, or network issues.
Error or Data Mishandling	Staff accidentally enter, delete, or improperly handle sensitive data.
Third-Party Breach	A vendor or partner system is compromised and exposes connected data.
Physical Theft of Equipment	Devices containing sensitive information are stolen or lost.
Outdated Procedures	Old or unmaintained processes create security gaps or compliance issues.
Temporary Connectivity Issues	Short-term internet or network disruptions limit system access.
Internet-Facing Threats	Internet threats from company services being accessible on the Internet.
Insider Threats	Malicious or negligent actions by employees, contractors, etc
Regulatory Changes	Changes in the regulatory landscape that may impact operations.

1. Risk Analysis

All risks identified will be assessed to identify the range of possible project outcomes. Risks will be prioritized by their level of importance.

a. Qualitative Risk Analysis

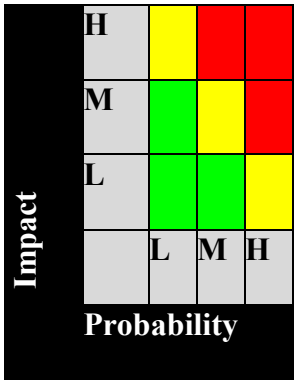
The probability and impact of occurrence for each identified risk will be assessed by the project manager, with input from the project team using the following approach:

Probability

- High – Greater than *<70%>* probability of occurrence
- Medium – Between *<30%>* and *<70%>* probability of occurrence
- Low – Below *<30%>* probability of occurrence

Impact

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
- Low – Risk that has relatively little impact on cost, schedule or performance



b. Qualitative Risk Analysis

Risks that fall within the red and yellow zones will have a detailed response plan that includes both a mitigation strategy and a contingency plan. Moderate risks will be reviewed periodically and mitigated as needed, while low risks will be monitored and reassessed in future reviews. This risk assessment uses a qualitative approach, categorizing probability and impact using descriptive ratings rather than numerical values.

Risk	Probability	Impact	Priority Level
Phishing/Malware	HIGH	HIGH	**CRITICAL**
Unauthorized Access to PHI	MEDIUM	HIGH	**HIGH**
Insider Threats	LOW	HIGH	**HIGH**
System or Network Failure	MEDIUM	MEDIUM	**MODERATE**
Error or Data Mishandling	MEDIUM	MEDIUM	**MODERATE**
Third-Party Breach	LOW	HIGH	**MODERATE**
Internet-Facing Threats	MEDIUM	MEDIUM	**MODERATE**
Power Outage	LOW	HIGH	**MODERATE**
Physical Theft of Equipment	LOW	MEDIUM	**LOW**
Outdated Procedures	LOW	LOW	**LOW**
Temporary Connectivity Issues	LOW	LOW	**LOW**
Regulatory Changes	LOW	LOW	**LOW**

2. Risk Response Planning

Each major risk identified in the red and yellow zones will be assigned to a specific risk owner responsible for monitoring and managing it throughout the project. This ensures accountability and prevents key risks from being overlooked. The response planning process focuses on reducing the likelihood and impact of the most critical risks while preparing contingency actions if they occur. Health Network Inc. will apply one or more of the following strategies for each risk:

Avoid: Eliminate the cause or exposure entirely.

Mitigate: Take proactive steps to reduce probability or impact.

Accept: Acknowledge the risk and prepare to manage consequences.

Contingency: Establish actions to take if the risk occurs.

Transfer: Shift the responsibility to another party (e.g., insurance, vendor contracts).

For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc. Any secondary risks that result from risk mitigation will be documented and follow the risk management protocol as the primary risks.

For each major risk that is to be mitigated or that is accepted, a course of action will be outlined if the risk does materialize in order to minimize its impact.

Phishing / Malware Attack - Critical

Response Strategy: Mitigate & Contingency
Actions: The IT and Security Staff will implement email filtering, conduct regular phishing awareness training, and perform simulated attack tests. Backup systems will be verified to ensure quick recovery if an incident occurs.

Unauthorized Access to PHI - High

Response Strategy: Mitigate
Actions: The Compliance Officer will enforce multi-factor authentication, perform regular access log reviews, and conduct quarterly audits of user permissions to prevent unauthorized access.

System or Network Failure - Moderate

Response Strategy: Contingency
Actions: The Chief Information Officer (CIO) will oversee redundancy implementation, ensure reliable data backups, and schedule semiannual disaster recovery tests to reduce downtime.

Data Mishandling / Human Error - Moderate

Response Strategy: Mitigate
Actions: Department Managers will provide ongoing training on PHI handling, secure data storage, and proper disposal methods. Regular internal audits will be conducted to ensure compliance with procedures.

Third-Party / Vendor Breach - Moderate

Response Strategy: Transfer & Mitigate
Actions: The Chief Executive Officer (CEO) will ensure that vendor contracts include strict HIPAA and HITRUST requirements. Vendor security assessments and insurance coverage will be reviewed annually.

Third-Party / Vendor Breach - Moderate

Response Strategy: Transfer & Mitigate
Actions: The Chief Executive Officer (CEO) will ensure that vendor contracts include strict HIPAA and HITRUST requirements. Vendor security assessments and insurance coverage will be reviewed annually.

Power Outage - Moderate

Response Strategy: Contingency
Actions: Executive Leadership, in coordination with the CIO, will maintain and routinely test backup power systems such as UPS and generators. These systems will be integrated into the organization's business continuity plan.

3. Controls

Health Network Inc. relies on a combination of administrative, technical, and physical controls to protect systems, maintain compliance, and reduce the likelihood of security incidents. These controls are designed to preserve the confidentiality, integrity, and availability of patient data while supporting daily healthcare operations.

Identify (ID):

1. An updated inventory of all hardware, software, and medical devices has been established and is maintained by IT staff.
2. Regular risk assessments and compliance reviews have been completed to identify and address organizational risks.
3. Third-party vendors have been evaluated for HIPAA and HITRUST compliance prior to onboarding.
4. **Covers:** Loss of company assets and Shadow IT risks, Regulatory & Compliance Changes, Third-Party Breach.

Protect (PR):

1. Role-based access control has been enforced, and password complexity requirements have been implemented across all systems.
2. Data encryption has been applied to all PHI in transit and at rest.
3. Annual HIPAA and cybersecurity awareness training has been conducted for all employees.
4. System patching and configuration management processes have been implemented and are regularly maintained.

5. Physical security measures, including keycard access and surveillance, have been enforced in data centers and administrative areas.
6. UPS systems and HVAC redundancy have been installed to protect against power and environmental failures.
7. **Covers:** Unauthorized Access to PHI, Insider Threats, Phishing/Malware and Error or Data Mishandling, Internet Threats and System Failure

Detect (DE):

1. Network activity has been continuously monitored using firewalls, antivirus software, and intrusion detection systems (IDS).
2. System and access logs have been regularly reviewed for unusual or suspicious activity.
3. Vulnerability scans and internal security audits have been performed on a recurring basis.
4. **Covers:** Malware, Internet-Facing Threats, Unauthorized Access, Outdated Procedures

Respond (RS):

1. A formal incident response plan has been developed and is actively followed during cybersecurity events.
2. Escalation procedures and communication channels have been defined and tested across departments.
3. Breach notification protocols have been enforced in coordination with compliance and leadership teams.

Recover (RC):

1. Encrypted backups have been created and stored both on-site and off-site for data protection.

2. Quarterly disaster recovery tests have been completed to verify system restoration capabilities.
3. The business continuity and recovery plans have been reviewed and updated annually to ensure readiness.

While Health Network Inc. maintains a solid security foundation, several controls should be added or strengthened to further align with the NIST Cybersecurity Framework (CSF), HITRUST CSF and improve overall resilience.

Identify (ID):

- Establish an asset classification process to label systems and data based on sensitivity and criticality.
- **Covers:** Data Mishandling

Protect (PR):

- Expand multi-factor authentication (MFA) to all users and systems handling PHI.
- Implement mobile device management (MDM) for secure remote access and data protection.

Detect (DE):

- Deploy a centralized Security Information and Event Management (SIEM) system for real-time monitoring.

Respond / Recover (RS–RC):

- Enhance the incident response plan with annual tabletop exercises and defined recovery metrics.

4. Roles and Responsibilities

To effectively manage risk, clear roles and responsibilities must be assigned throughout the organization. At Health Network Inc., risk management is a shared responsibility, with leadership setting direction and oversight, and all employees contributing to the protection of sensitive data and systems.

- **Executive Leadership**
    - Provide strategic oversight of risk management initiatives.
    - Approve the risk management plan and allocate necessary resources.
    - Ensure organizational compliance with federal and state laws (HIPAA, HITECH) and industry frameworks (HITRUST, PCI DSS).
- **Chief Executive Officer (CEO)**
    - Holds ultimate accountability for risk management within the organization.
    - Ensures risk management objectives align with business goals and patient care priorities.
    - Serves as the executive sponsor for compliance certifications
- **Chief Information Officer (CIO)**
    - Oversee IT operations and ensure systems support organizational objectives.
    - Coordinates with the CISO to align IT practices with security and compliance requirements.
    - Ensures that new technologies and vendors are evaluated for risk prior to adoption.

- **Compliance Officer**
    - Ensures compliance with HIPAA, HITECH, and other healthcare specific regulations.
    - Coordinates audits, documentation, and regulatory reporting.
- **Department Managers (Clinical, Financial, etc.)**
    - Ensure staff within their departments follow established security policies and procedures.
    - Identify department-specific risks and report them to leadership.
- **IT and Security Staff**
    - Implement, monitor, and maintain technical controls.
    - Conduct system patching, vulnerability management, and incident response.

5. Schedule

The risk management plan will be completed in four parts according to the project timeline. Each part builds on the previous deliverables to ensure a structured and comprehensive final plan. The schedule is as follows:

Part #	Description	Due Date
1.	Draft of the introduction, scope and boundaries, compliance laws/regulations, and roles/responsibilities	9/28
2.	Draft of Risk Assessment Plan, including risk identification, identified threats and vulnerabilities, Qualitative Risk Analysis, Response planning, and controls.	10/19
3.	Risk mitigation plan, including known threats, new threats, controls to mitigate, and possible future threats to the organization	11/9
4.	Business Impact Analysis (BIA) & Business Continuity Plan (BCP), including estimated impacts and downtime.	11/23
5.	**Final draft of the Risk Management Plan**	12/11

Part 3 – Risk Mitigation Plan

1. Introduction

The risk mitigation plan outlines how Health Network Inc. will reduce or eliminate risks that could disrupt operations, compromise patient information, or impact clinical services. This section builds on the findings from the risk assessment and provides a focused approach to maintaining secure and reliable systems across the organization.

2. Purpose and Importance

The purpose of this plan is to describe the actions the organization will take to manage identified risks, strengthen defenses, and support safe workflows. This plan is important because it ensures that risk reduction is intentional, documented, and aligned with compliance requirements such as HIPAA and HITRUST. By following a structured mitigation process, the organization can prevent avoidable disruptions, reduce the chance of data loss, and improve overall readiness for security incidents.

3. Previously Identified Threats

Identified Threat/Vulnerability	Overview of Threat/Vulnerability
Phishing/Malware	Attackers trick staff into clicking harmful links or files that compromise systems or data.
Unauthorized Access to PHI	Someone gains access to patient information without proper permissions.
System or Network Failure	Critical systems stop working due to hardware, software, or network issues.
Error or Data Mishandling	Staff accidentally enter, delete, or improperly handle sensitive data.
Third-Party Breach	A vendor or partner system is compromised and exposes connected data.
Physical Theft of Equipment	Devices containing sensitive information are stolen or lost.
Outdated Procedures	Old or unmaintained processes create security gaps or compliance issues.
Temporary Connectivity Issues	Short-term internet or network disruptions limit system access.
Internet-Facing Threats	Internet threats from company services being accessible on the Internet.
Insider Threats	Malicious or negligent actions by employees, contractors, etc
Regulatory Changes	Changes in the regulatory landscape that may impact operations.

4. Newly Identified Threats

During continued review, additional risks emerged that were not initially documented. These include misconfigured or unmonitored cloud services, insider misuse of access privileges, insecure remote connections, outdated or unpatched medical devices, vulnerabilities in vendor-supplied software, and weak password hygiene among staff. These threats were identified through system scans, workflow observation, and policy audits, showing that risks evolve as technology and operations change.

5. Controls to Implement

To reduce the risks identified during the assessment, Health Network Inc. will implement targeted security controls aligned with NIST 800-53. These controls focus on strengthening authentication, tightening access permissions, improving monitoring, and securing both internal systems and third-party connections. Additional measures include enhanced staff training, stricter configuration and patch management, secure remote access, and stronger protections for backups, cloud services, and medical devices.

Identified Control Need	NIST 800-53 Control(s)	Description
Misconfigured or unmonitored cloud services	SC-7, SC-28, SA-5	Requires boundary protection, encryption of cloud data, and secure acquisition/configuration of cloud services.
Insider misuse of access privileges	AC-6, AU-6, PS-3, PS-6	Enforces least privilege, monitors user actions, and evaluates personnel in trusted roles.
Insecure remote connections	AC-17, AC-17(2), IA-2(1)	Requires secure remote access channels and MFA for remote sessions.
Outdated or unpatched medical devices	SI-2, SI-3, CM-8	Ensures timely patching, anti-malware protections, and accurate tracking of device inventory.
Vulnerabilities in vendor-supplied software	SA-9, SR-3, SR-5	Requires assessment of vendor security, supply-chain risk management, and continuous monitoring.
Weak password hygiene among staff	IA-5, AT-2	Establishes strong password rules and user training to reduce credential misuse.

6. Future Threats

As Health Network Inc. continues to grow and bring in new systems, more risks will naturally appear. These could include smarter phishing attacks using AI, new zero-day flaws in medical devices, weaknesses in cloud apps or telehealth platforms, and ransomware that targets backups instead of just servers. Third-party service failures, software bugs from vendors, and security issues tied to remote work or personal devices could also become bigger problems over time. As the environment changes, so do the ways attackers try to get in, so staying aware of these shifting risks is important.

To keep up with these future threats, the organization will rely on regular vulnerability scans, penetration testing, and configuration audits to catch technical issues early. Continuous SIEM monitoring and alerting will help flag unusual activity, while threat intelligence feeds, healthcare security bulletins, and H-ISAC updates will provide warnings about new attack methods. Annual risk assessments, vendor reviews, system upgrade checks, and staff feedback will help spot risks introduced by new tools or workflow changes. This ongoing process makes sure the organization can quickly identify, evaluate, and respond to any new threats that show up.

Part 4 – Business Impact Analysis (BIA) & Business Continuity Plan (BCP)

Business Impact Analysis

A. Purpose

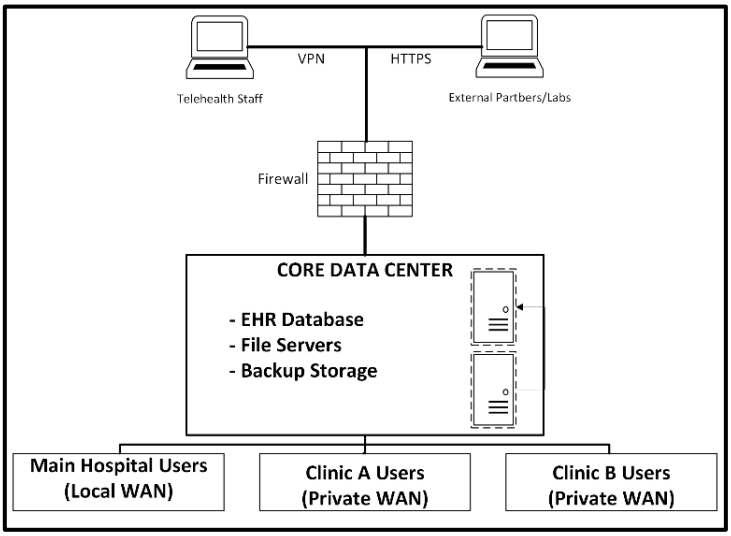
- *Mission/Business Processes and Recovery Criticality*
  - Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.

- *Resource Requirement*
  - 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.

- *Recovery Priorities*
  - 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.

B. System Descriptions

Health Network Inc. relies on the EHR system to handle all essential daily tasks, including patient charting, admissions, and billing. This system functions on servers located physically within the secure data center at the organization's headquarters. Staff members at the main hospital and satellite clinics access the system through the internal network, while authorized remote employees connect securely using a VPN. The system also interfaces with external partners, such as laboratories and insurance companies, to share medical results and process payments. To ensure business continuity and recovery, the organization performs nightly encrypted backups of all data to a secure off-site cloud storage location.



C. Determine Process and System Criticality

Working with input from department managers, clinical staff, and IT leadership, the following mission critical processes have been identified. These processes rely heavily on the availability of the data center and EHR system and the underlying network infrastructure.

Mission/Business Process	Description
Clinical Documentation & Patient Care	The continuous process of recording patient vitals, medical history, diagnoses, and treatment plans in the EHR during active care. This is the primary function of the organization.
Patient Admissions & Registration	The intake process for new and returning patients, including insurance verification, demographic entry, and assigning patients to beds or providers.
Pharmacy & Medication Administration	The electronic verification of prescriptions (e-prescribing) and the "five rights" checking (right patient, right drug, etc.) before administering medication to ensure safety.
Telehealth Services	Remote video consultations between providers and patients, which rely on secure network connections and the patient portal interface.
Pay Vendor Invoices	The financial process of obligating funds, issuing checks or electronic payments to suppliers
Laboratory Order & Result Processing	Transmitting orders to labs and test results back into the patient's electronic chart for diagnosis.
Insurance Claims Processing	Submitting medical claims to payers to ensure the organization receives reimbursement for services.

If criticality of mission/business processes has not been determined outside of the BIA, the following subsections will help to determine criticality of mission/business processes that depend on or support the information system.

D. Outage Impacts

This section defines what "bad" looks like for the organization. In healthcare, we look at three main areas: Patient Safety (the most critical), Financial/Legal (money and laws like HIPAA), and Public Image (trust).

Impact Category: Patient Safety & Quality of Care

- **Severe =** Potential for loss of life or permanent injury; inability to treat emergency patients; total loss of access to critical patient history (allergies, meds).
- **Moderate =** Significant delays in treatment; reliance on manual paper charting increases risk of errors; diversion of ambulances to other facilities.
- **Minimal =** Rescheduling of elective procedures; minor administrative delays; non-urgent workflow inconveniences.

Impact Category: Financial & Compliance

- **Severe =** Revenue loss exceeding $100,000 per day; significant HIPAA violation fines (> $50,000); loss of insurance accreditation.
- **Moderate =** Increased operational costs due to staff overtime for manual data entry; minor regulatory reporting delays; revenue delayed by > 1 week.
- **Minimal =** Minor late fees on vendor payments (< $1,000); cost of office supplies for paper downtime procedures.

Impact Category: Public Image & Reputation

- **Severe =** National media coverage of the outage/breach; loss of major partners or community trust; significant patient churn.
- **Moderate =** Local news coverage; increased volume of patient complaints on social media.
- **Minimal =** Internal staff frustration; no public awareness of the issue.

The table below summarizes the impact on each mission/business process if the data center were unavailable.

Mission/Business Process	Impact Category			
	Safety	**Financial**	**Reputation**	**Impact**
Documentation & Patient Care	Severe	Moderate	Moderate	CRITICAL
Patient Admissions & Registration	Severe	Moderate	Minimal	HIGH
Medication Administration	Moderate	Moderate	Moderate	CRITICAL
Telehealth Services	Minimal	Moderate	Moderate	MODERATE
Pay Vendor Invoices	Minimal	Minimal	Minimal	LOW
Laboratory Order & Result Processing	Moderate	Moderate	Minimal	HIGH
Insurance Claims Processing	Minimal	Severe	Minimal	MODERATE

E. 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 (MTD): The MTD 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 MTD 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 MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

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 MTD, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on the data center.

Mission/Business Process	Downtime (Hours)		
	MDT	**RTO**	**RPO**
Documentation & Patient Care	24	4	0.25
Patient Admissions & Registration	48	24	1
Medication Administration	24	4	1
Telehealth Services	72	48	4
Pay Vendor Invoices	168	72	24
Laboratory Order & Result Processing	24	8	1
Insurance Claims Processing	168	72	24

Identify Resource Requirements

The following table identifies the resources that compose the data center including hardware, software, and other resources such as data files.

System Resource/Component	Platform/OS/Version	Description
EHR Database Server	Windows Server 2022 / SQL Server 2019	The primary database server hosting all patient records (PHI) and historical data.
Application Server	Windows Server 2022	Runs the core EHR software logic and handles user requests from clinics and the hospital.
Web Server	Windows Server 2022 / IIS 10.0	Hosts the internal web interface and the external-facing Patient Portal.
Network Core Switch	Cisco Catalyst 9000 Series	The main network backbone connecting the Data Center to the hospital floors and clinics.
Firewall Appliance	Palo Alto Networks PA-3200	Provides perimeter security, VPN access for remote staff, and intrusion prevention.
Clinical Workstations	Windows 11 Enterprise	Desktop computers used by nurses and doctors for charting and data entry.
Backup Storage Array	Dell EMC PowerStore	Dedicated local storage hardware for housing encrypted nightly backups.

F. Identify Recovery Priorities for System Resources

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

Priority	System Resource/Component	RTO
1	Network Core Switch & Firewall	2 Hours
2	EHR Database Server	4 Hours
3	Application Server	4 Hours
4	Web Server	8 Hours
5	Clinical Workstations	24 Hours
6	Backup Storage Array	24 Hours

Business Continuity Plan (BCP)

A. Overview

The Health Network Inc. Business Continuity Plan (BCP) establishes the procedures required to maintain critical operations during a significant disruption. The primary objective is to ensure patient safety and the continuity of care, even if the HealthNet Core EHR and other technical systems are unavailable. This plan is activated when a disruption exceeds the established Recovery Time Objectives (RTO) or when executive leadership deems it necessary to protect organizational interests.

I. Scope

This plan applies to all Health Network Inc. facilities, including the main hospital campus, satellite clinics, and administrative offices. It covers all personnel, clinical staff, and third-party contractors who support critical business functions. The plan specifically addresses the loss of the EHR system, network connectivity, and power infrastructure.

II. Key Business Areas

The following functions have been prioritized for continuity efforts based on the Business Impact Analysis (BIA):

1. **Patient Care & Clinical Documentation:** Ensuring medical history and treatment plans are accessible and updated.
2. **Admissions & Registration:** Processing new patients safely.
3. **Medication Administration:** Verifying and dispensing prescriptions without electronic safety checks.
4. **Internal Communication:** Coordinating staff response across departments.

III. Critical Functions

To ensure patient safety and organizational stability during a disruption, Health Network Inc. prioritizes the recovery and manual support of the following operations:

1. **Emergency & Inpatient Care:** The immediate treatment of life-threatening conditions in the ER and ICU.
2. **Pharmacy Services:** The verification and dispensing of medications to prevent adverse drug events
3. **Surgical Services:** The execution of emergency and time-sensitive surgeries
4. **Patient Admissions:** The intake and tracking of patients to ensure they are routed to the correct care providers.
5. **Diagnostics (Lab & Imaging):** Processing essential blood work and scans required for immediate diagnosis.
6. **Support:** Maintaining power, medical gases (oxygen), and HVAC systems necessary for a safe clinical environment.

IV. Acceptable Downtime

While the IT Recovery Time Objective (RTO) for the EHR is 4 hours, clinical operations cannot pause. Therefore, zero downtime is acceptable for patient care. Manual backup procedures must be implemented immediately (within 15 minutes) of a confirmed system outage to ensure no interruption in service.

V. Plan to Maintain Operations

In the event of a system failure, the organization will transition to Standard Downtime Procedures:

- **Clinical Operations (Paper Charting):**

    - "Downtime Crash Carts" containing paper forms (Admission, Vitals, Progress Notes, Prescription Pads) are located at every nursing station.
    - Staff will manually record all patient interactions on these forms.
    - Historical patient data (allergies/history) will be accessed via the "Shadow Read-Only" backup computers located in the ER, which update nightly and operate independently of the main network.
- **Admissions:**
    - Patient intake will be performed using paper registration packets.
    - Staff will manually apply wristbands using the standalone downtime label printers.
- **Pharmacy:**
    - Runners will physically transport paper medication orders from nursing units to the pharmacy.
    - Pharmacists will manually verify dosages and dispense medications using the local inventory override mode.

B. Roles and Responsibilities

Incident Management Team (IMT)

- **Incident Commander (CEO):** Declares the disaster, authorizes the move to downtime procedures, and manages overall strategy.
- **Operations Lead (Chief Medical Officer):** Oversees clinical quality and safety during manual operations.
- **Logistics Lead (Facilities Manager):** Ensures supply of paper forms, food, and fuel for generators.

- **Technical Lead (CIO):** Focuses solely on system restoration and estimates recovery time.

C. Emergency Communications

- **Primary:** Mass Notification System (Text/Email blast) to all employees alerting them to "Code Gray" (IT System Failure).
- **Secondary:** Departmental "Call Trees" where managers manually call their staff if email is down.

D. Customer Communications

- Notices will be posted at all physical entrances explaining potential wait times.
- A banner will be placed on the public website with status updates.

E. Staff Communications

- Hourly briefings will be held at the Command Center (Conference Room B).
- Runners will distribute printed status updates to nursing stations every 4 hours.

F. Incident Response Procedures

1. **Activation:** The Help Desk receives multiple reports of outages. The CIO confirms the issue and advises the CEO. The CEO activates the BCP
2. **Notification:** The "Code Gray" alert is sent. Department managers open Downtime Crash Carts.
3. **Manual Operations:** Clinical staff begin paper charting. Non-critical appointments are rescheduled.
4. **Recovery:** IT restores systems. Once verified stable, the "All Clear" is given.

5. **Data Entry (Catch-up):** Staff are assigned overtime to manually enter data from the paper forms back into the EHR system.

G. Plan Testing and Maintenance

To ensure this plan works when needed, Health Network Inc. will conduct the following tests.

- **Tabletop Exercises (Annually):** The Incident Management Team meets to talk through a hypothetical scenario (e.g., "Ransomware Attack") to identify gaps in decision-making.
- **Functional Drills (Semi-Annually):** Specific departments (e.g., ER) will simulate a 1-hour downtime, using paper forms for actual patients to ensure staff remain familiar with manual processes.
- **Call Tree Validation (Quarterly):** Managers will test contact numbers to ensure staff lists are up to date.
- **Plan Review:** The BCP will be reviewed and updated annually or after any significant IT infrastructure changes

References

1 Cybersecurity Risk Management and Information Protection | HITRUST. (2025). Retrieved September 30, 2025, from Hitrustalliance.net website: https://hitrustalliance.net/

2 Cybersecurity Framework | NIST. (2013, November 12). Retrieved September 30, 2025, from NIST website: https://www.nist.gov/cyberframework

3 Office. (2008, May 7). Summary of the HIPAA Privacy Rule. Retrieved September 30, 2025, from HHS.gov website: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

4 Leni Sagita Riantini Supriadi, & Pheng, L. S. (2017). Business Continuity Management (BCM). Management in the Built Environment, 41–73. https://doi.org/10.1007/978-981-10-5487-7_3