

**2024 NIST CSF 2.0 Annual Risk Assessment**  
  
**Review Type:** 2024 NIST CSF 2.0 Annual Risk Assessment

**Completion:** MM/DD/YYY

**Policy Area:** Information Security Risk Management Policy and Procedure

**Applicability:** Organization Company-wide

BLANK PAGE



SUMMARY

The Information Security Team is pleased to present this overview of the annual Heath New England (HNE) NIST CSF 2.0 Risk Assessment. NIST Cyber Security Framework (NIST CSF) is a framework that is used for the protection of sensitive information (e.g., PHI, PII, and our commitment to information security necessitates a thorough evaluation of potential risks to the confidentiality, integrity, and availability of protected health information.

This report provides insight into the objectives and the methodology of our NIST CSF risk assessment. We aim to identify and analyze risks and ensuring our security measures align with HIPAA regulations. Through this assessment, we aim to not only meet regulatory requirements but also to fortify our organization's security posture and enhance the overall protection of PHI.

**We encourage all stakeholders to review this report, as it lays the foundation for ongoing efforts to mitigate risks, maintain compliance, and continuously improve our security measures. We appreciate your collaboration and commitment to safeguarding the privacy and security of health information.**



Contents

[Executive Summary 5](#_Toc171062655)

[Objectives 6](#_Toc171062656)

[Scope of the Assessment 6](#_Toc171062657)

[Risk Assessment Methodology 6](#_Toc171062658)

[Summary of Identified Gaps 7](#_Toc171062659)

[Report Summary 9](#_Toc171062660)

[Appendix A: Detailed Gaps 10](#_Toc171062661)

[Appendix B: Threats and Vulnerabilities per Gap 22](#_Toc171062662)

[Appendix C: Interview/Survey Contact List 34](#_Toc171062663)

[Appendix D: NIST CSF 2.0 and HIPAA Crosswalk 35](#_Toc171062664)

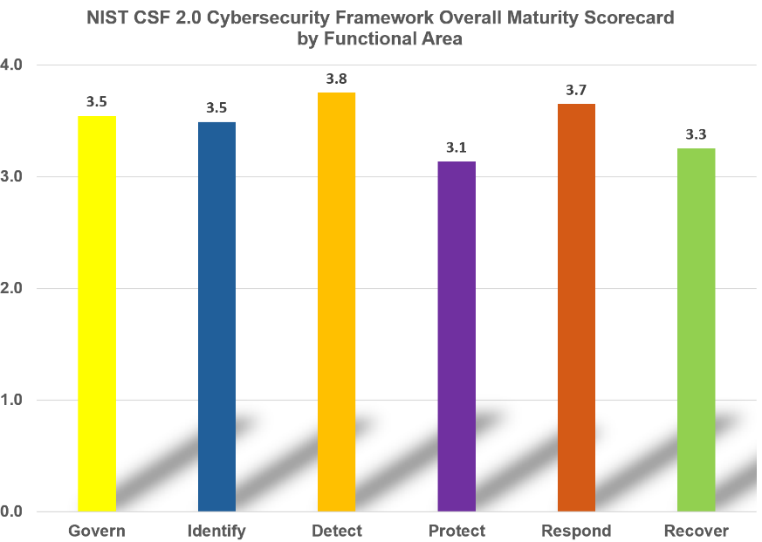
[Appendix E: Defining NIST CSF 2.0 Tiering 38](#_Toc171062665)

[Appendix F: Tactical and Strategic Roadmaps 40](#_Toc171062666)

[Appendix G: NIST CSF Subdomain Scorecard 41](#_Toc171062667)



# Executive Summary



The Information Security Team is pleased to present this overview of the annual NIST Cybersecurity Framework (NIST CSF) 2.0 Risk Assessment. The Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of sensitive health information. HNE uses the NIST CSF to identify risks and mitigation strategies to reduce risks of adverse events. HNE requires a thorough evaluation of potential risks to the confidentiality, integrity, and availability of protected health information (PHI).

This report provides insight into the objectives and methodology of our NIST CSF risk assessment. We aim to identify and analyze risks while ensuring our security measures align with HIPAA regulations. Through this assessment, we aim to not only meet regulatory requirements but also to fortify our organization's security posture and enhance the overall protection of PHI. In addition, this document will roadmap the tactical and strategic plan.

From May to July of 2024, HNE conducted a NIST CSF risk assessment looking at 107 controls to create a baseline for an acceptable level of security to identify risks. Maturity is based on a 1 - 4 scale as defined on the NIST CSF Tiering definitions used as a rubric. See *Defining NIST CSF 2.0 Tiering in Appendix E* to see the definitions. Overall, HNE scored a 3.4 out of 4. Though there are areas of improvement for some of the NIST CSF Subcategories the score and maturity of each subcategory illustrates an effective security program.

There were twenty-two (22) Gaps noted. There were 0 critical, 3 high, 13 medium, and 6 low. See the [*Detailed*](#_Detailed_Findings) *Gap in Appendix A* below for more information about each discovered gap.

We encourage all stakeholders to review this report, as it lays the foundation for ongoing efforts to mitigate risks, minimize adverse impacts, maintain compliance, and continuously improve our security measures. We appreciate your collaboration and commitment to safeguarding the privacy and security of health information.

# Objectives

The primary objectives of the Annual HNE NIST CSF risk assessment are to:

* Discover and document potential risks to the security of PHI using an industry standard framework.
* Identify threats and vulnerability to each gap identified.
* Assess the potential impact and likelihood of identified gap.
* Ensure that the organization's policies and procedures align with HIPAA requirements.
* Identify gaps in the current security measures.
* Develop strategies and action plans to mitigate and manage identified risks effectively.
* Develop a tactical and strategic roadmap.

# Scope of the Assessment

The scope of the NIST CSF 2.0 analysis focuses on asset and data management, ensuring that inventories of hardware, software, and critical assets are up-to-date, and that sensitive patient data is appropriately classified and protected. Implementing robust identity and access management controls, encrypting data both at rest and in transit, and securing all platforms, including cloud services, are necessary protective measures. Continuous monitoring for irregular activity, analyzing incidents to understand their impact, and recovery planning to ensure timely restoration of normal operations, with communication to relevant stakeholders. Furthermore, managing cybersecurity risks associated with suppliers, including contractual provisions for incident response, providing regular employee training on cybersecurity, and regularly auditing and assessing practices to ensure compliance and identify improvement areas are critical components of the scope

# Risk Assessment Methodology

In conducting the Annual NIST CSF risk assessment, information was gathered from several sources to understand and evaluate HNE’s security landscape against NIST CSF. The process began with identifying all ePHI information systems, networks, hardware, software, and personnel. The assessment attempts to identify potential threats, malicious attacks, and technical failures by a lack of proper security controls. Simultaneously, vulnerabilities in systems and processes are assessed, often involving thorough reviews of configurations, penetration testing results, and an analysis of existing security controls. The effectiveness of current security measures, such as access controls, encryption, and incident response procedures, is also evaluated.

The assessment followed the guidelines and standards outlined in the HIPAA Security Rule and NIST CSF for guidance in safeguarding PHI. Additionally, regulatory compliance requirements pertinent to HNE’s operations were considered, ensuring alignment with HIPAA/NIST CSF. The process incorporated interviews with key stakeholders, documentation reviews, and analyses of historical data, including past security assessments and pen testing reports. The culmination of this information allowed for a holistic understanding of HNE’s risk landscape, and facilitating informed decision-making for risk prioritization and mitigation strategies.

Emphasizing a holistic security management process, NIST CSF delves into key components such as risk assessment, policy development, workforce training, and ongoing monitoring. NIST CSF sheds light on technical safeguards, including access controls, audit controls, and integrity controls, offering insights into their implementation and maintenance to secure electronic health information.

The methodology followed the following steps:

1. **Organizational Context**

* Gain an understanding of the business mission
* Gain an understanding of Stakeholder expectations
* Legal, regulatory, and contractual requirements
* Dependencies (critical objectives, capabilities, and services)

1. **Current Cybersecurity Profile (Posture)**

* Document the current status of each subcategory, providing a detailed assessment of the organization’s current cybersecurity capabilities

1. **Gap Analysis**

* Compare the current and target profiles to identify areas needing improvement
* Document specific gaps in each function, category, and subcategory

1. **Develop Plan of Action and Milestone (POA&Ms)**

* Outline steps to address the identified gaps
* Assign responsibilities, resources, and timelines for each action item

1. **Future Cybersecurity Profile (Posture) [Strategic Plan]**

* Define the desired outcomes for each function, category, and subcategory
* Prioritize these outcomes based on risk

1. **Continuous Monitoring**

* Ensure all POA&Ms are tracked to closure
* Ensure all current controls remain adequate

1. **Define Performance Measures**

* Define key performance indicators (KPIs) and metrics to track progress
* Establish a process for regularly reviewing and updating the profile

# Summary of Identified Gaps

| **Risk Rating** | **Gaps** | **Action Steps to Mitigate** |
| --- | --- | --- |
| **HIGH** | There is ePHI production data in the test environment [§164.312(a)(1), §164.312(b), §164.312(c)(1)] | Review if HNE will remove ePHI data from test or put compensating controls around the test environment to make it similar to the production environment. |
| **HIGH** | MFA missing on some internet facing web applications [§164.312(a)(1), §164.312(d)] | MFA is on the Tactical Information Security Roadmap to be remediated over the next 12 months. |
| **HIGH** | Logs are not being captured for all critical ePHI systems. Logs are being captured from security solutions. HNE’s security solutions do not contain ePHI. Log monitoring and regular reviews are part of ensuring compliance with this requirement to detect and address any unauthorized access to ePHI. [§164.312(b)] | Review the following systems to identify if it’s technically possible to send security logs (e.g., failed logons) to the SEIM: Edifecs, HNEDirect, Amisys, CARE, Change Healthcare, Claims Xten, ComCom, Cypress, Docustream, Enrollment HUB, MultiPlan, Northwood, OptumHealth, Amazon Web Services |

| **Risk Rating** | **Gaps** | **Action Steps to Mitigate** |
| --- | --- | --- |
| **MEDIUM** | Amisys has PHI and there are only two roles in Amisys. A user role and an admin role. PHI is not restricted to users that have a need-to-know basis. The CP038POL Confidentiality of System Security Information states, "It is HNE’s policy to limit access to and disclosure of HNE’s System Security Information to those who have a legitimate need to know the information in order to perform the specific functions of their jobs" In addition, there is prod data in test. {§164.312(a)(1)} | Create a plan for the implementation of RBAC on Amysis system and determine how to build RBAC into critical ePHI systems, where the technical feasibility. |
| **MEDIUM** | The incident response (IR) policy and procedure needs to be updated to include {§164.308(a)(6)(i)} | Update and enhance the Incident Response Policy and SOPs. Document Who needs to be notified, how to communicate, and when, include guidelines that specify what information will be shared, with whom, under what circumstances, and through what channels, ensure there are logs or records that detail the information shared with stakeholders, including the date, the type of information, the recipient, and the purpose of sharing, critical third parties must be involved in incident response testing and IR policy should state when an incident is completed, communicated, and closed |
| **MEDIUM** | HNE does not have an updated Business Continuity plan {§164.308(a)(7)(i)} | The BCP/BIA are currently being updated |
| **MEDIUM** | HNE does not review 3rd Party security certifications (e.g., SOC 2 Type 2, HITRUST), if available. {§164.308(a)(1)(ii)(A)} | When doing vendor reviews, ask to see an attestation of an industry information security program certification (HITRUST, SOC 2), if available. Ensure the certification is applicable to the service being requested by HNE. |
| **MEDIUM** | Clear passwords in text file on network server {§164.312(a)(1)} | The user IDs and passwords are being integrated into Delinia PAM solution. |
| **MEDIUM** | Flat network / Non-segmented network {§164.312(a)(1)} | There is a current project to develop micro-segmentation. |
| **MEDIUM** | Limited security architectural and data flow diagrams documentation {§164.308(a)(1)(ii)(B)} | Documentation of the architectural and data flow diagrams are currently underway. |
| **MEDIUM** | Data retention and destruction process {§164.502(b)} | Design and implement a data retention and destruction process. |
| **MEDIUM** | Limited standards for consistent control implementation {§164.312(c)(1)} | Develop and implement system configuration standards for critical ePHI business application and security tools to ensure consistent implementation. |
| **MEDIUM** | There is not a comprehensive guide provided to all developers that outlines required security practices, such as input validation, encryption of sensitive data, and error handling. There needs to be developer training on creating secure code. There is no code scanning (SAST or DAST) {§164.312(c)(1)} | Implement continuous security code reviews (e.g., using a tool called SafeOps) |
| **MEDIUM** | There is no role-based access control for the Amysis environment {§164.312(a)(4)(ii)(B)} | Where technically feasible, review and implement RBAC for ePHI systems |
| **MEDIUM** | There is no capturing of cyber threat intelligence from information sharing forums and sources to monitor our critical third parties {§164.312(a)(1)(ii)(A), §164.312(a)(1)(ii)(B), §164.312(a)(1)(ii)(D), §164.312(b)(1)} | Implement third party cybersecurity intelligence to identify incidents (e.g., H-ISAC) |

# Report Summary

Overall, Health New England demonstrates an effective information security program.

# Appendix A: Detailed Gaps

| **Observation** | **Subcategory** | **Risk Statement** | **How to Mitigate** | **Current Mitigation Actions** | **Risk Level** |
| --- | --- | --- | --- | --- | --- |
| HNE has ePHI production data in the test environment | PR.DS-01  PR.DS-02 | Using electronic protected health information (ePHI) production data in the test environment can lead to unauthorized access and exposure of sensitive patient information. This practice increases the risk of data breaches, violates regulatory compliance requirements, and can result in significant financial penalties, loss of patient trust, and reputational harm to the organization | Data de-identification is essential, involving techniques such as anonymization, pseudonymization, and data masking to ensure that data cannot be traced back to individuals. Alternatively, synthetic data that mimics the statistical properties of real data can be used. Access controls, including strict authorization measures and role-based access control (RBAC), should be established to limit access to ePHI. Additionally, isolating test environments from production environments and employing network segmentation can prevent data cross-contamination and control access effectively | Needs to be discussed for a decision of how to mitigate. Will the risk be transferred, mitigated, or accepted | **HIGH** |
| MFA missing on some internet facing web applications | PR.AA-03  ID.RA-05 | Absence of multi-factor authentication (MFA) on internet-facing applications significantly increases the risk of unauthorized access and cyberattacks. This vulnerability can lead to data breaches, exposure of sensitive information, regulatory non-compliance, substantial financial losses, and severe damage to the organization's reputation and trustworthiness | First and foremost, deploying MFA across all internet-facing applications is crucial. This added layer of security ensures that only authorized users can access sensitive information and critical systems | Externally facing web applications are being updated to include MFA | **HIGH** |
| Logs are not being captured for all critical ePHI systems. Logs are being captured from security solutions. HIPAA §164.312(b) states that all required covered entities implement hardware, software and/or procedure mechanisms that record (log) and examine (audit) activity in information systems that contain or use electronic protected heath information (ePHI).  HNE’s security solutions do no contain ePHI. Log monitoring and regular reviews are part of ensuring compliance with this requirement to detect and address any unauthorized access to ePHI. | DE.CM-01 | Not having centralized security logs can lead to fragmented and incomplete visibility of security events across the organization. This may result in delayed detection and response to security incidents, increased vulnerability to cyberattacks, compliance violations, and potentially severe financial and reputational damage due to undetected or unresolved security breaches. The following systems are not sending log data to Exabeam, Amisys, Edifecs, HNEDirect, CARE, Claims Xten, ComCom, Cypress, Docustream, Enrollment HUB | Implement a centralized logging system that aggregates security logs from all critical systems and applications. This centralized approach ensures comprehensive visibility of security events across the organization, enabling quicker detection and response to potential security incidents. By consolidating logs into a single system, security teams can more efficiently monitor, analyze, and correlate events, which helps in identifying patterns and anomalies indicative of cyberattacks. Regularly maintaining and auditing this centralized log system ensures that it remains effective and that logs are collected consistently from all relevant sources. | Logs are being assessed to discover which logs, if technically feasible, go to the SEIM. There are currently 8 feeds going into the SIEM, which are security tool feeds, but none are critical ePHI systems. | **HIGH** |
| Amisys has PHI and there are only two roles in amisys. A user role and an admin role. PHI is not restricted to users that have a need-to-know basis. The CP038POL Confidentiality of System Security Information states, "It is HNE’s policy to limit access to and disclosure of HNE’s System Security Information to those who have a legitimate need to know the information in order to perform the specific functions of their jobs" In addition, there is prod data in test | PR.DS-10 | There is a risk that unauthorized access or misuse of the Amysis system could occur due to insufficiently defined or enforced access control between the Admin and User roles. This could lead to the exposure, alteration, or loss of critical ePHI data, compromising patient confidentiality, integrity, and availability | Design alternative controls, strengthen authentication mechanisms, enhance RBAC, continuous monitoring and auditing by sending logs to the SIEM, user training and awareness, and incident response planning specific to Amysis | Needs to be discussed for a decision of how to mitigate. Will the risk be transferred, mitigated, or accepted | **MEDIUM** |
| HIPAA §164.308(a)(6)(i) states that covered entities must implement policies and procedures to address security incidents. The standard specifically mandates the identification and response to suspected or known security incidents, mitigating their harmful effects, and documenting incidents and their outcomes in an orderly fashion. The incident response (IR) policy and procedure needs to be updated to include who needs to be notified, how to communicate, and when in the when in the event of an incident. In addition, the IR policy needs to be update to include guidelines that specify what information will be shared, with whom, under what circumstances, and through what channels. Furthermore, ensure there are logs or records that detail the information shared with stakeholders, including the date, the type of information, the recipient, and the purpose of sharing. Next, The IR policy, SOP, and playbooks, need documentation on how recovery actions are planned, including criteria for selecting, scoping, and prioritizing these actions. In addition, critical third parties must be involved in incident response testing.  Finally, the IR policy should state when an incident is completed, communicated, and closed. | GV.SC-01  GV.SC-02  GV.SC-08  GV.SC.09 | An incomplete incident response program can result in delayed identification, containment, and mitigation of security incidents. This may lead to prolonged data breaches, increased damage to information systems, non-compliance with regulatory requirements, significant financial losses, and erosion of stakeholder trust and organizational reputation | Update the incident response plan | Incident response plans and incident SOPs are currently being update in accordance with the BCP/BIA updates | **MEDIUM** |
| HNE does not have an updated Business Continuity plan as per §164.308(a)(7)(i) which states, "Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information." In addition to prevention, the goal is to enable ongoing operations before and during the execution of disaster recovery. Business continuity is the intended outcome of properly executing business continuity planning and disaster recovery. With a Business Continuity Plan, HNE will know how to keep the business going during an adverse incident | GV.OC-04 | Absence of a formal Business Continuity Program and a comprehensive Business Impact Risk Analysis may result in prolonged operational disruptions and an inability to promptly restore critical healthcare services during emergencies or disasters. This can lead to significant patient care delays, financial losses, non-compliance with regulatory requirements, and diminished organizational reputation | To ensure the effectiveness of a Business Continuity Program (BCP) and Business Impact Analysis (BIA), healthcare organizations must prioritize regular updates and revisions. This involves continuously monitoring and reviewing both the BCP and BIA to identify areas for improvement. Lessons learned from actual incidents and drills should be incorporated to enhance the plans. | Business Continuity Plans and Business Impact Assessments are being updated currently. | **MEDIUM** |
| Third Party Risk Management. §164.308(a)(1)(ii)(A) - Requires entities to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity or business associate Terms of Services are not reviewed. HNE does not review 3rd Party security certifications, if available. | RS.MA-01 | Failure to conduct a comprehensive risk analysis on third-party vendors that handle protected health information (PHI) may result in unauthorized access, data breaches, and non-compliance with HIPAA regulations, potentially leading to significant financial penalties, reputational damage, and loss of patient trust. | To mitigate this risk, HNE should collect, if available, a security certification, such as SOC 2 Type 2, HITRUST CSF, ISO 27001. | Needs to be discussed for a decision of how to mitigate. Will the risk be transferred, mitigated, or accepted | **MEDIUM** |
| Clear passwords in text file on network server | PR.AT-01 | Storing clear text passwords in a text file on a shared server significantly increases the risk of unauthorized access to sensitive systems and data. This practice can lead to security breaches, data theft, non-compliance with regulatory standards, substantial financial losses, and severe reputational damage to the organization | The clear text passwords and user ids need to put into the PAM solution. | Add the user IDs and password to Delinea Privileged Access Management (PAM) Tool | **MEDIUM** |
| Flat network / Non-segmented network | PR.IR-01 | Having a flat network with no network segmentation can lead to increased vulnerability to cyberattacks, as a single compromised device can provide attackers with unfettered access to the entire network. This lack of segmentation can result in widespread data breaches, unauthorized access to sensitive information, regulatory non-compliance, significant financial losses, and severe damage to the organization's reputation | Implement network segmentation. By dividing the network into smaller, isolated segments, organizations can limit the spread of cyberattacks and reduce the impact of a single compromised device. Each segment can be secured independently, ensuring that sensitive information and critical systems are protected even if one part of the network is breached. This approach not only helps in containing potential data breaches but also improves overall network performance and security | Micro-segmentation project | **MEDIUM** |
| There is no comprehensive review of access control for systems that process, transmit, or store ePHI on a specified frequency. Lack of access control reviews could lead to a potential past employee or a current transfer employee having more access than they need or having access after they leave HNE | PR.AA-04 | Failure to regularly review and update access controls in electronic protected health information (ePHI) systems may result in unauthorized access, misuse, or data breaches. This can lead to compromised patient confidentiality, regulatory non-compliance, substantial financial penalties, loss of patient trust, and significant reputational damage to the organization | Each critical system must have its access reviewed by the owner of the system, or delegate. Access controls lists should be sent to each critical system owner to ensure that the access is appropriate and attested. | Needs to be discussed for a decision of how to mitigate. Will the risk be transferred, mitigated, or accepted | **MEDIUM** |
| Limited security architectural and data flow diagrams documentation | ID.AM-06 | The absence of security architectural and data flow diagrams can result in an incomplete understanding of the system’s security posture and data movement. This lack of visibility may lead to undetected vulnerabilities, inefficient incident response, non-compliance with regulatory requirements, potential data breaches, and significant financial and reputational damage | Ensure to develop an [architectural](https://creately.com/guides/data-architecture-diagram-tutorial/#:~:text=Best%20Practices%20for%20Drawing%20Data%20Architecture%20Diagrams%201,and%20Flexibility%20...%207%20Leverage%20Software%20Features%20) and data flow diagram. | The architectural and data diagram are currently being developed. | **MEDIUM** |
| Data retention and destruction process | PR.DS-08  PR.DS-09 | Absence of a formal data retention and destruction process can lead to the improper handling of sensitive information, resulting in unauthorized access, data breaches, and non-compliance with regulatory requirements. This can cause significant legal and financial penalties, reputational damage, and loss of stakeholder trust. | Develop a program that documents identifies critical data sets, determine how long critical data sets should be kept, for example 7, 10, 25 years, etc, then implement controls to delete data after the retention period is over. | Needs to be discussed for a decision of how to mitigate. Will the risk be transferred, mitigated, or accepted | **MEDIUM** |
| Limited standards for consistent control implementation | PR.PS-01 | Limited or no security configuration standards for managing can result in inconsistent application of security controls, leaving systems vulnerable to unauthorized access and data breaches. This inconsistency can lead to regulatory non-compliance, increased risk of security incidents, significant financial losses, and damage to the organization's reputation | Develop security standards to ensure consistency of security controls configuration implementation. This will ensure that any security practitioner to implement the security controls consistently. For example, when setting up a SIEM solution, and a security practitioner finds another job outside HNE, the next security practitioner can implement the same controls in the same manner. | Needs to be discussed on how to do this, as well as who will do it. | **MEDIUM** |
| There is not a comprehensive guide provided to all developers that outlines required security practices, such as input validation, encryption of sensitive data, and error handling. There needs to be developer training on creating secure code. There is no code scanning (SAST or DAST) | PR.PS-06 | Not implementing a code scanning review to detect potential vulnerabilities can result in the deployment of insecure applications. This lack of proactive vulnerability management increases the risk of security breaches, data exposure, regulatory non-compliance, substantial financial losses, and significant damage to the organization's reputation | Implement a program to scan critical code. Identify and mitigate vulnerabilities prior to deployment into the production environment. | Current discussions on bringing in a code scanning solution, possible Rapid 7 | **MEDIUM** |
| There is no role-based access control for the Amysis environment | PR.AA-05 | Absence of role-based access control for an electronic protected health information (ePHI) system can result in unauthorized access to sensitive patient data. This lack of access control increases the risk of data breaches, misuse of information, regulatory non-compliance, substantial financial penalties, and significant damage to the organization's reputation and trust | Determine how RBAC can be deployed in critical systems, such as Amysis, for come up with mitigating controls around critical applications. | Given the acquisition position, this risk may be accepted. However, if not accepted, then a discussion need to be conducted to figure out mitigating actions. | **MEDIUM** |
| There is no capturing of cyber threat intelligence from information sharing forums and sources to monitor our critical third parties | ID.RA-02  DE.CM-06 | The risk of not monitoring third parties for breaches could lead to undetected security incidents within the supply chain, resulting in the unauthorized access, disclosure, or loss of sensitive data. This lack of visibility into third parties security posture could compromise the overall security of the organization and its data. | Continuous monitoring of third parties through intelligence services like H-ISAC or Prevalent.net. Develop an incident response collaboration between critical third parties to create a trusted relationship | Needs to be discussed for a decision of how to mitigate | **MEDIUM** |
| Job descriptions help identify particular skills or abilities necessary for a given position. There is a lack of Job Descriptions that specifically state what data a user can access, for example, ePHI. This will help IT determine what systems they are allowed to access. | GV.RR-02 | Failing to define appropriate data access requirements in job descriptions can lead to employees having unauthorized or excessive access to sensitive information. This oversight increases the risk of data exposure, misuse of information, regulatory non-compliance, potential financial losses, and damage to the organization's reputation and trust | In the JDs, add a line that this role can have access to PHI and/or ePHI. | Needs to be discussed for a decision of how to mitigate | **LOW** |
| There are no Policy communication when updates are made | GV.PO-01  ID.IM-03  RS.CO-02 | Failure to effectively communicate updates to policies and standards to employees can lead to non-compliance with current security protocols and regulatory requirements. This lack of awareness may result in increased risk of security breaches, operational inefficiencies, potential legal and financial penalties, and damage to the organization's reputation and trustworthiness. | When updates to policies are completed, a communication should go out to the affected workforce members to ensure they understand what change affected their organizations. | Needs to be discussed for a decision of how to mitigate | **LOW** |
| The Customer Service Management system is running on an outdated and unsupported MS Access database | PR.PS-02 | MS Access has reached end-of-life as of October 13, 2020. Using MS Access without access controls to store CSM information can lead to unauthorized access, data exposure, and misuse of potential sensitive customer data. This risk increases the possibility of regulatory non-compliance, substantial financial loses, loss of customer trust, and potential dame to the organizations reputation. | Put controls around the access database to prevent unauthorized access to the CSM system | Needs to be discussed for a decision of how to mitigate | **LOW** |
| There is no targeted training for certain job roles that could impact security. For example, and IT Admin should be trained on how to secure their systems or be able to identify anomalies | PR.AT-02 | Not providing targeted information security training for different roles within the organization can lead to inadequate understanding of security practices and procedures. This one-size-fits-all approach may result in inefficient use of training time, increased risk of security incidents, regulatory non-compliance, and potential data breaches. Ultimately, it can cause significant financial losses, operational disruptions, and damage to the organization's reputation | Determine the different groups that require targeted training. Use KB4 to group workforce members. Send targeted training. | Needs to be discussed for a decision of how to mitigate | **LOW** |
| There is no exception policy or process when policies deviations occur. High & Critical need to go to senior management to approve. | ID.RA-07 | No having a exception policy or process could lead to unmanaged and undocumented deviations from established policies. This could result in vulnerabilities being introduced into the organization’s environment, increasing the risk of security incidents and data breaches | Establish an exception policy and process. Ensure there is a hierarchical process for critical and high risk changes. Ensure there is due diligence documentation for auditing purposes. Ensure there are regular reviews of exceptions an organizational defined frequency to check if the exception is still needed. | Needs to be discussed for a decision of how to mitigate | **LOW** |
| Ensure IR Policy, SOP, and playbooks, have documentation on how recovery actions are planned, including criteria for selecting, scoping, and prioritizing these actions.  Ensure there are procedures in the SOP and Playbooks that outline how the integrity of backups and restoration assets is checked, including the tools and methods used  Create a section in the IR SOP, that mentions how polcy and organizational adjustments will be made.  Add functions that verify the integrity of the restored assest and update the SOP  Create criteria that specify what conditions must be met to declare the end of an incident recovery, including system checks, security verifications, and business operations assessments in the SOP.  Develop guidelines that specify what information should be shared, with whom, under what circumstances, and through what channels | RC.RP-02  RC.RP-03  RC.RP-04  RC.RP-05  RC.RP-06 | Not regularly checking backups and restoration procedures after an incident, not documenting how policies will be adjusted after incidents, not clearly defining when an incident has ended, and lack of sharing and communicating could lead to prolonged downtime, data loss, data access, and inadequate incident response. These deficiencies could exacerbate the impact of cybersecurity incidents, resulting in significant operational, financial, and reputational damage to the organization. | Ensure there are regular backup testing before and after an incident. Make adjustments to policies and SOPs. Clear statement on when the incident is concluded. Ensure there are clear communication protocols laid out in the Policy. Ensure there is a post-mortem analysis. Ensure there is specific training and awareness. | Needs to be discussed for a decision of how to mitigate | **LOW** |

# Appendix B: Threats and Vulnerabilities per Gap

| **Observation** | **Subcategory** | **Risk Statement** | **Threats** | **Vulnerabilities** | **Risk Level** |
| --- | --- | --- | --- | --- | --- |
| HNE has ePHI production data in the test environment | PR.DS-01  PR.DS-02 | Using electronic protected health information (ePHI) production data in the test environment can lead to unauthorized access and exposure of sensitive patient information. This practice increases the risk of data breaches, violates regulatory compliance requirements, and can result in significant financial penalties, loss of patient trust, and reputational harm to the organization | Data breaches, unauthorized access, malware attacks, insider threats, physical theft, ransomware, data tampering. | Improper access controls, lack of monitoring, poor data management policies, insufficient incident response. | **HIGH** |
| MFA missing on some internet facing web applications | PR.AA-03  ID.RA-05 | Absence of multi-factor authentication (MFA) on internet-facing applications significantly increases the risk of unauthorized access and cyberattacks. This vulnerability can lead to data breaches, exposure of sensitive information, regulatory non-compliance, substantial financial losses, and severe damage to the organization's reputation and trustworthiness | Credential Theft, Brute Force Attack, Insider Threats, Man-in-the-Middle (MITM) Attacks, Phishing Attacks, Exploitation of Weak Authentication Protocols | Weak password policies, single factor authentication, unpatached software, Lack of MFA, inadequate user education, insecure storage credentials, lack of monitoring and logging | **HIGH** |
| Logs are not being captured for all critical ePHI systems. Logs are being captured from security solutions. HIPAA §164.312(b) states that all required covered entities implement hardware, software and/or procedure mechanisms that record (log) and examine (audit) activity in information systems that contain or use electronic protected heath information (ePHI).  HNE’s security solutions do no contain ePHI. Log monitoring and regular reviews are part of ensuring compliance with this requirement to detect and address any unauthorized access to ePHI. | DE.CM-01 | Not having centralized security logs can lead to fragmented and incomplete visibility of security events across the organization. This may result in delayed detection and response to security incidents, increased vulnerability to cyberattacks, compliance violations, and potentially severe financial and reputational damage due to undetected or unresolved security breaches. The following systems are not sending log data to Exabeam, Amisys, Edifecs, HNEDirect, CARE, Claims Xten, ComCom, Cypress, Docustream, Enrollment HUB | Unauthorized access, network attacks, malware, insider threats, data breaches, DDoS attacks, man-in-the-middle attacks | Inadequate monitoring tools, poor network visibility, lack of real-time monitoring, outdated security protocols, insufficient logging, lack of trained personnel | **HIGH** |
| Amisys has PHI and there are only two roles in amisys. A user role and an admin role. PHI is not restricted to users that have a need-to-know basis. The CP038POL Confidentiality of System Security Information states, "It is HNE’s policy to limit access to and disclosure of HNE’s System Security Information to those who have a legitimate need to know the information in order to perform the specific functions of their jobs" In addition, there is prod data in test | PR.DS-10 | There is a risk that unauthorized access or misuse of the Amysis system could occur due to insufficiently defined or enforced access control between the Admin and User roles. This could lead to the exposure, alteration, or loss of critical ePHI data, compromising patient confidentiality, integrity, and availability | Insider threats, unauthorized access, malware, data tampering, process hijacking, data leaks, exploitation of vulnerabilities | Insecure processing environments, lack of monitoring, insufficient access controls, outdated systems, weak application security, poor data handling practices, inadequate encryption | **MEDIUM** |
| HIPAA §164.308(a)(6)(i) states that covered entities must implement policies and procedures to address security incidents. The standard specifically mandates the identification and response to suspected or known security incidents, mitigating their harmful effects, and documenting incidents and their outcomes in an orderly fashion. The incident response (IR) policy and procedure needs to be updated to include who needs to be notified, how to communicate, and when in the when in the event of an incident. In addition, the IR policy needs to be update to include guidelines that specify what information will be shared, with whom, under what circumstances, and through what channels. Furthermore, ensure there are logs or records that detail the information shared with stakeholders, including the date, the type of information, the recipient, and the purpose of sharing. Next, The IR policy, SOP, and playbooks, need documentation on how recovery actions are planned, including criteria for selecting, scoping, and prioritizing these actions. In addition, critical third parties must be involved in incident response testing.  Finally, the IR policy should state when an incident is completed, communicated, and closed. | GV.SC-01  GV.SC-02  GV.SC-08  GV.SC.09 | An incomplete incident response program can result in delayed identification, containment, and mitigation of security incidents. This may lead to prolonged data breaches, increased damage to information systems, non-compliance with regulatory requirements, significant financial losses, and erosion of stakeholder trust and organizational reputation | Supply chain disruptions, unmanaged risks, stakeholder conflicts | Lack of supply chain risk management program, poor strategy alignment, inadequate stakeholder agreement | **MEDIUM** |
| HNE does not have an updated Business Continuity plan as per §164.308(a)(7)(i) which states, "Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information." In addition to prevention, the goal is to enable ongoing operations before and during the execution of disaster recovery. Business continuity is the intended outcome of properly executing business continuity planning and disaster recovery. With a Business Continuity Plan, HNE will know how to keep the business going during an adverse incident | GV.OC-04 | Absence of a formal Business Continuity Program and a comprehensive Business Impact Risk Analysis may result in prolonged operational disruptions and an inability to promptly restore critical healthcare services during emergencies or disasters. This can lead to significant patient care delays, financial losses, non-compliance with regulatory requirements, and diminished organizational reputation | Service disruptions, loss of stakeholder trust, unmet stakeholder expectations | Inadequate understanding of critical services, poor communication of capabilities, insufficient service continuity planning | **MEDIUM** |
| Third Party Risk Management. §164.308(a)(1)(ii)(A) - Requires entities to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity or business associate Terms of Services are not reviewed. HNE does not review 3rd Party security certifications, if available. | RS.MA-01 | Failure to conduct a comprehensive risk analysis on third-party vendors that handle protected health information (PHI) may result in unauthorized access, data breaches, and non-compliance with HIPAA regulations, potentially leading to significant financial penalties, reputational damage, and loss of patient trust. | Cyber attacks, data breaches, malware, insider threats, service disruptions, supply chain attacks, unauthorized access | Poor incident response planning, lack of coordination with third parties, insufficient communication channels, inadequate incident documentation, weak access controls, outdated response protocols, insufficient resources | **MEDIUM** |
| Clear passwords in text file on network server | PR.AT-01 | Storing clear text passwords in a text file on a shared server significantly increases the risk of unauthorized access to sensitive systems and data. This practice can lead to security breaches, data theft, non-compliance with regulatory standards, substantial financial losses, and severe reputational damage to the organization | Social engineering attacks, phishing attacks, insider threats, lack of awareness, credential theft, human error, spear phishing | Insufficient training programs, outdated training materials, lack of engagement, infrequent training, lack of role-specific training, poorly defined objectives, ineffective delivery methods | **MEDIUM** |
| Flat network / Non-segmented network | PR.IR-01 | Having a flat network with no network segmentation can lead to increased vulnerability to cyberattacks, as a single compromised device can provide attackers with unfettered access to the entire network. This lack of segmentation can result in widespread data breaches, unauthorized access to sensitive information, regulatory non-compliance, significant financial losses, and severe damage to the organization's reputation | Unauthorized access, data breaches, malware, insider threats, network attacks, system compromise, exploitation of vulnerabilities | Weak access controls, insufficient network segmentation, poor monitoring, outdated security protocols, inadequate logging, lack of multi-factor authentication, insufficient training | **MEDIUM** |
| There is no comprehensive review of access control for systems that process, transmit, or store ePHI on a specified frequency. Lack of access control reviews could lead to a potential past employee or a current transfer employee having more access than they need or having access after they leave HNE | PR.AA-04 | Failure to regularly review and update access controls in electronic protected health information (ePHI) systems may result in unauthorized access, misuse, or data breaches. This can lead to compromised patient confidentiality, regulatory non-compliance, substantial financial penalties, loss of patient trust, and significant reputational damage to the organization | Interception of identity assertions, replay attacks, man-in-the-middle attacks, forgery of identity assertions, credential stuffing, session hijacking, exploitation of weak verification protocols | Unencrypted transmission, lack of token expiry, weak encryption algorithms, insufficient validation checks, insecure storage, inadequate monitoring, poor session management | **MEDIUM** |
| Limited security architectural and data flow diagrams documentation | ID.AM-06 | The absence of security architectural and data flow diagrams can result in an incomplete understanding of the system’s security posture and data movement. This lack of visibility may lead to undetected vulnerabilities, inefficient incident response, non-compliance with regulatory requirements, potential data breaches, and significant financial and reputational damage | Unauthorized access, malware, insider threats, phishing and social engineering, data leakage, supply chain compromise, network attacks, system misconfigurations, DoS | Weak access controls, outdated or unpatached software, weak authentication mechanisms, insufficient data encryption and loss prevention controls, poor network segmentation and inadequate firewall configuration audits, insufficient bandwidth or lack of DoS mitigation strategies. | **MEDIUM** |
| Data retention and destruction process | PR.DS-08 | Absence of a formal data retention and destruction process can lead to the improper handling of sensitive information, resulting in unauthorized access, data breaches, and non-compliance with regulatory requirements. This can cause significant legal and financial penalties, reputational damage, and loss of stakeholder trust. | Unauthorized data recovery, improper data disposal techniques, dumpster diving, insider threats | Lack of data destruction policies and standards, inadequate training on data disposal, weak physical security controls, insufficient monitoring of disposal process. | **MEDIUM** |
| Limited standards for consistent control implementation | PR.PS-01 | Limited or no security configuration standards for managing can result in inconsistent application of security controls, leaving systems vulnerable to unauthorized access and data breaches. This inconsistency can lead to regulatory non-compliance, increased risk of security incidents, significant financial losses, and damage to the organization's reputation | Unauthorized changes, misconfigurations, malware, insider threats, system failures, exploitation of vulnerabilities, data breaches | Lack of configuration policies, inadequate change management, insufficient monitoring, outdated systems, poor documentation, lack of training, weak access controls | **MEDIUM** |
| There is not a comprehensive guide provided to all developers that outlines required security practices, such as input validation, encryption of sensitive data, and error handling. There needs to be developer training on creating secure code. There is no code scanning (SAST or DAST) | PR.PS-06 | Not implementing a code scanning review to detect potential vulnerabilities can result in the deployment of insecure applications. This lack of proactive vulnerability management increases the risk of security breaches, data exposure, regulatory non-compliance, substantial financial losses, and significant damage to the organization's reputation | Software vulnerabilities, unauthorized access, malware, code injection attacks, insider threats, supply chain attacks, software tampering | Inadequate secure development practices, insufficient code review, lack of security testing, poor version control, inadequate developer training, weak access controls, outdated development tools | **MEDIUM** |
| There is no role-based access control for the Amysis environment | PR.AA-05 | Absence of role-based access control for an electronic protected health information (ePHI) system can result in unauthorized access to sensitive patient data. This lack of access control increases the risk of data breaches, misuse of information, regulatory non-compliance, substantial financial penalties, and significant damage to the organization's reputation and trust | Unauthorized access, privilege escalation, insider threats, access control policy violations, weak separation of duties, exploitation of excessive privileges | Outdated access control policies, improperly configured access controls, lack of audit and review, inadequate role-based access control, failure to implement least privilege, insufficient user training. | **MEDIUM** |
| There is no capturing of cyber threat intelligence from information sharing forums and sources to monitor our critical third parties | ID.RA-02  DE.CM-06 | The risk of not monitoring third parties for breaches could lead to undetected security incidents within the supply chain, resulting in the unauthorized access, disclosure, or loss of sensitive data. This lack of visibility into third parties security posture could compromise the overall security of the organization and its data. | Emerging threats, sophisticated cyber attacks, insider threats, data breaches, service disruptions, malware, unauthorized access | Lack of threat intelligence sources, inadequate information sharing, insufficient monitoring, poor access controls, outdated threat management processes, weak incident response plans, inadequate training | **MEDIUM** |
| Job descriptions help identify particular skills or abilities necessary for a given position. There is a lack of Job Descriptions that specifically state what data a user can access, for example, ePHI. This will help IT determine what systems they are allowed to access. | GV.RR-02 | Failing to define appropriate data access requirements in job descriptions can lead to employees having unauthorized or excessive access to sensitive information. This oversight increases the risk of data exposure, misuse of information, regulatory non-compliance, potential financial losses, and damage to the organization's reputation and trust | Role confusion, unmanaged risks, lack of accountability | Undefined roles and responsibilities, poor communication, inadequate enforcement | **LOW** |
| There are no Policy communication when updates are made | GV.PO-01  ID.IM-03  RS.CO-02 | Failure to effectively communicate updates to policies and standards to employees can lead to non-compliance with current security protocols and regulatory requirements. This lack of awareness may result in increased risk of security breaches, operational inefficiencies, potential legal and financial penalties, and damage to the organization's reputation and trustworthiness. | Non-compliance, unmanaged risks, policy violations | Lack of clear policies, poor communication, inadequate enforcement | **LOW** |
| The Customer Service Management system is running on an outdated and unsupported MS Access database | PR.PS-02 | MS Access has reached end-of-life as of October 13, 2020. Using MS Access without access controls to store CSM information can lead to unauthorized access, data exposure, and misuse of potential sensitive customer data. This risk increases the possibility of regulatory non-compliance, substantial financial loses, loss of customer trust, and potential dame to the organizations reputation. | Vulnerability exploitation, outdated software, malware, unauthorized access, insider threats, system failures, data breaches | Lack of update policies, inadequate patch management, insufficient monitoring, outdated software, poor inventory management, lack of testing, weak access controls | **LOW** |
| There is no targeted training for certain job roles that could impact security. For example, and IT Admin should be trained on how to secure their systems or be able to identify anomalies | PR.AT-02 | Not providing targeted information security training for different roles within the organization can lead to inadequate understanding of security practices and procedures. This one-size-fits-all approach may result in inefficient use of training time, increased risk of security incidents, regulatory non-compliance, and potential data breaches. Ultimately, it can cause significant financial losses, operational disruptions, and damage to the organization's reputation | Specialized phishing attacks, insider threats, social engineering attacks, lack of awareness, targeted malware, inadequate incident response, exploitation of role-specific vulnerabilities | Inadequate role-specific training, outdated content, lack of continuous updates, insufficient threat awareness, poor understanding of policies, limited access to resources, weak collaboration. | **LOW** |
| There is no exception policy or process when policies deviations occur. High & Critical need to go to senior management to approve. | ID.RA-07 | No having a exception policy or process could lead to unmanaged and undocumented deviations from established policies. This could result in vulnerabilities being introduced into the organization’s environment, increasing the risk of security incidents and data breaches | Unauthorized access, data breaches, malware, insider threats, service disruptions, sophisticated cyber attacks, data loss | Poor change and exception management, inadequate risk impact assessments, insufficient recording and tracking, weak access controls, lack of incident response plans, outdated risk management policies, inadequate training | **LOW** |
| Ensure IR Policy, SOP, and playbooks, have documentation on how recovery actions are planned, including criteria for selecting, scoping, and prioritizing these actions.  Ensure there are procedures in the SOP and Playbooks that outline how the integrity of backups and restoration assets is checked, including the tools and methods used  Create a section in the IR SOP, that mentions how polcy and organizational adjustments will be made.  Add functions that verify the integrity of the restored assest and update the SOP  Create criteria that specify what conditions must be met to declare the end of an incident recovery, including system checks, security verifications, and business operations assessments in the SOP.  Develop guidelines that specify what information should be shared, with whom, under what circumstances, and through what channels | RC.RP-02  RC.RP-03  RC.RP-04  RC.RP-05  RC.RP-06 | Not regularly checking backups and restoration procedures after an incident, not documenting how policies will be adjusted after incidents, not clearly defining when an incident has ended, and lack of sharing and communicating could lead to prolonged downtime, data loss, data access, and inadequate incident response. These deficiencies could exacerbate the impact of cybersecurity incidents, resulting in significant operational, financial, and reputational damage to the organization. | Data loss, service disruptions, malware, insider threats, unauthorized access, system failures, supply chain attacks | Poor recovery action selection, inadequate prioritization, insufficient documentation, lack of monitoring, weak access controls, outdated response protocols, insufficient resources | **LOW** |

# Appendix C: Interview/Survey Contact List

|  |  |
| --- | --- |
| **Workforce Member** | **Role** |
| Ashley Bogle | Legal |
| Charmalee Tulloch | Compliance |
| Gary Kellums | Infrastructure |
| Charmalee Tulloch | Compliance |
| Jason Rio | CRO |
| William Stoner | IT Core apps |
| Walter Gadomski | Application Development |
| Jack Costa | Network |
| Venkataramana Kamireddy | Enterprise IT |
| Ranga |  |
|  |  |

# Appendix D: NIST CSF 2.0 and HIPAA Crosswalk

This crosswalk aligns the controls and requirements of the NIST Cybersecurity Framework (CSF) 2.0, NIST SP 800-66, and the HIPAA Security Rule to help organizations understand how these frameworks and regulations interrelate and support compliance and risk management.

1. **Govern (GV) Function**

| **CSF 2.0 Subcategory** | **CSF 2.0 Subcategory Definition** | **HIPAA Security Rule** |
| --- | --- | --- |
| **GV.OC - Organizational Context** | GV.OC-01: Organizational mission informs cybersecurity risk management | §164.306(a)(2): Protect against any reasonably anticipated threats or hazards |
| **GV.RM - Risk Management Strategy** | GV.RM-01: Risk management strategy defined and implemented | §164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks |
| **GV.RR - Roles, Responsibilities, and Authorities** | GV.RR-01: Roles and responsibilities defined | §164.308(a)(2): Identify the security official responsible for the development of security policies |
| **GV.PO - Policy** | GV.PO-01: Policy established and communicated | §164.316(a): Implement reasonable and appropriate policies and procedures |
| **GV.OV - Oversight** | GV.OV-01: Oversight of cybersecurity risk management activities | §164.308(a)(1)(ii)(D): Regularly review records of information system activity |
| **GV.SC - Cybersecurity Supply Chain Risk Management** | GV.SC-01: Cybersecurity supply chain risk management processes established | §164.308(b)(1): Ensure that all business associates comply with the security rule |

2. Identify (ID) Function

| **CSF 2.0 Subcategory** | **CSF 2.0 Subcategory Definition** | **HIPAA Security Rule** |
| --- | --- | --- |
| ID.AM – Asset Management | ID.AM-01: Physical devices and systems within the organization are inventoried | §164.310(d)(2)(iii): Maintain an inventory of hardware |
| ID.RA – Risk Assessment | ID.RA-01: Asset vulnerabilities identified and documented | §164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of risks |
| ID.IM – Improvement | ID.IM-01: Continuous improvement through lessons learned | §164.308(a)(8): Perform a periodic technical and non-technical evaluation |

3. Protect (PR) Function

| **CSF 2.0 Subcategory** | **CSF 2.0 Subcategory Definition** | | **HIPAA Security Rule** |
| --- | --- | --- | --- |
| PR.AA – Identity Management, Authentication, and Access Control | PR.AA-01: Identities and credentials are issued, managed, verified, and revoked | §164.312(a)(1): Implement technical policies and procedures for access control | |
| PR.AT – Awareness and Training | PR.AT-01: Awareness and training programs conducted | §164.308(a)(5)(i): Implement a security awareness and training program | |
| PR.PS – Platform Security | PR.DS-01: Data at rest is protected | §164.312(e)(1): Implement technical security measures to guard against unauthorized access to data | |
| PR.PS – Platform Security | PR.PS-01: Security of software platforms and applications is managed | §164.310(b): Implement policies and procedures regarding workstation use | |
| PR.IR – Technology Infrastructure Resilience | PR.IR-01: Technology infrastructure is resilient | §164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore lost data | |

4. Detect (DE) Function

| **CSF 2.0 Subcategory** | **CSF 2.0 Subcategory Definition** | | **HIPAA Security Rule** | | |
| --- | --- | --- | --- | --- | --- |
| DE.CM – Continuous Monitoring | | DE.CM-01: Networks are monitored to detect potential cybersecurity events | | §164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in systems |
| DE.AE – Adverse Event Analysis | | DE.AE-01: Adverse events are analyzed to understand their impact | | §164.308(a)(6)(ii): Identify and respond to suspected or known security incidents |

5. Respond (RS) Function

| **CSF 2.0 Subcategory** | **CSF 2.0 Subcategory Definition** | | **HIPAA Security Rule** | |
| --- | --- | --- | --- | --- |
| RS.MA – Incident Management | RS.MA-01: Incidents are managed to minimize impact | §164.308(a)(6)(ii): Identify and respond to suspected or known security incidents | |
| RS.AN – Incident Analysis | RS.AN-01: Incidents are analyzed to determine their effect on the organization | §164.308(a)(6)(ii): Mitigate, to the extent practicable, harmful effects of security incidents | |
| RS.CO – Incident Response Reporting and Communication | RS.CO-01: Reporting processes are established | §164.308(a)(6)(ii): Document security incidents and their outcomes | |
| RS.MI – Incident Mitigation | RS.MI-01: Corrective actions are identified and implemented | §164.308(a)(7)(ii)(C): Implement procedures for data backup and recovery | |

6. Recover (RC) Function

| **CSF 2.0 Subcategory** | | **CSF 2.0 Subcategory Definition** | | **HIPAA Security Rule** | |
| --- | --- | --- | --- | --- | --- |
| RC.RP – Incident Recovery Plan Execution | RC.RP-01: Recovery plans are executed to restore systems | | §164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore lost data | |
| RC.CO – Incident Recovery Communication | RC.CO-01: Recovery activities are communicated to internal stakeholders | | §164.308(a)(7)(ii)(D): Conduct periodic testing and revision of contingency plans | |

# Appendix E: Defining NIST CSF 2.0 Tiering

The Tiering in the NIST CSF 2.0 are the levels of the cybersecurity management rigor within HNE, ranging from Tier 1 (Partial) to Tier 4 (Adaptive). These tiers characterize the sophistication and maturity of HNE’s cyber security practices, with higher tiers indicating more advanced, integrated, and continuously improving the cybersecurity management approaches. The tiers are used as a rubric when assessing security controls. Below defines the NIST CSF 2.0 Tiering definitions.

**Tier 1 – Partial:**

Application of the organizational cybersecurity risk strategy is managed in an ad hoc manner. Prioritization is ad hoc and not formally based on objectives or threat environment. There is limited awareness of cybersecurity risks at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis. The organization may not have processes that enable cybersecurity information to be shared within the organization. The organization is generally unaware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses

**Tier 2 – Risk Informed**

Risk management practices are approved by management but may not be established as organization-wide policy. The prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements. There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring. Cybersecurity information is shared within the organization on an informal basis. The organization is aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks

**Tier 3 – Repeatable**

The organization’s risk management practices are formally approved and expressed as policy. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape. There is an organization-wide approach to managing cybersecurity risks. Cybersecurity information is routinely shared throughout the organization. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors the cybersecurity risks of assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risks. Executives ensure that cybersecurity is considered through all lines of operation in the organization. The organization risk strategy is informed by the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Personnel formally act upon those risks through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. These actions are implemented consistently and as intended and are continuously monitored and reviewed

**Tier 4 – Adaptive**

There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. Executives monitor cybersecurity risks in the same context as financial and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture. It evolves from an awareness of previous activities and continuous awareness of activities on organizational systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated. The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats. The organization uses real-time or near real-time information to understand and consistently act upon the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Cybersecurity information is constantly shared throughout the organization and with authorized third parties.

# Appendix F: Tactical and Strategic Roadmaps



Insert Strategic Roadmap

# Appendix G: NIST CSF Subdomain Scorecard

