|  |  |  |
| --- | --- | --- |
| **Policy Number**:  **Policy Area**:  **Line of Business**:  **Effective Date**:  **Reviewed Date**:  **Replaces Policy**: | ITSEC002PGM  Information Security  Corporate  02/01/2017  04/05/2024  N/A | Health New England Brand |
| Information Security Management Program (ISMP) | | |

**Purpose**

The purpose of this Program is to ensure that the established Health New England’s (HNE) Information Security Management (ISMP) Program is properly and effectively managed through monitoring, maintenance, and improvement. The ~~purpose of this Program~~ ISMP is to establish administrative, technical, and physical safeguards to protect Personal Health Information (PHI) and Personal Information (PI) that is owned, licensed, stored, or maintained by HNE, whether such Information is contained in paper or electronic records or in any other form. This ~~Program~~ ISMP is designed to ensure the security and confidentiality of PHI and PI ~~Personal Information~~, to protect against anticipated threats or hazards to the security or integrity of PHI and PI ~~Personal Information~~, and to protect against unauthorized access to or use of PHI and PI ~~Personal Information~~ in a manner that creates a substantial risk of identity theft or fraud. Finally, the ISMP is also considered our Written Information Security Program document in accordance with The Commonwealth of Massachusetts Privacy Law.

**Scope**

This policy applies to all workforce members whether full-time, part-time, independent contractors, consultants, volunteers, and interns of HNE and its subsidiaries

**Policy**

~~In order to implement and properly maintain a robust Information Security Program, HNE follows these principles:~~

* ~~Understanding HNE’s information security requirements and the need to establish policy and objectives for information security~~
* ~~Implementing and operating controls to manage HNE’s information security risks in the context of overall business risks~~
* ~~Ensuring all users of HNE information assets are aware of their responsibilities in protecting those assets~~
* ~~Monitoring and reviewing the performance and effectiveness of information security policies and controls~~
* ~~Continual improvement based on assessment, measurement, and changes that affect risk~~

The objective of the Information Security Management Program is to provide management direction and support for information security in accordance with business requirements and governing laws and regulations. Information security policies will be approved by management, and published and communicated to all employees and relevant external parties. These policies will set Health New England’s approach to managing information security and will align with relevant company policies.

Information security policies will be reviewed annually or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. Each policy will have an owner who has approved management responsibility for the development, review, and evaluation of the policy. Reviews will include assessing opportunities for improvement of information security policies and approach to managing information security in response to changes in environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

It is recognized no set of controls will achieve complete security. Additional management action will be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls to support HNE goals and objectives.

**Sanctions**

Non-Compliance. Instances of non-compliance with the ISMP must be reported immediately to the Manager, MA Data Privacy Coordinator, Human Resources Department and the Chief Information Security Officer. Violations may result in disciplinary action by HNE, up to and including termination of employment.

Non-Retaliation. It is unlawful and against HNE policy to retaliate against anyone who reports a violation of this Program or who cooperates in an investigation regarding non-compliance with this Program. Any such retaliation will result in disciplinary action by HNE, up to and including termination of employment.

**Procedure**

The following are components of the Information Security Program that will be managed:

1. **Risk Management**

Risk Management refers to the process of identifying risk, assessing risk, and ~~taking steps to reduce~~ mitigate risk to an acceptable level. Risk management is critical to successfully implement and maintain a secure environment. Risk assessments will identify, quantify, and prioritize risks against business criteria for risk acceptance and objectives. The results will guide the tactical and strategic plan a~~nd determine appropriate action and priorities for managing information security risks and for implementing controls needed to protect information assets.~~

Risk management will include the following steps as part of a risk assessment:

1. Use a risk management framework to review controls against current processes and control implementation
2. Identify the risks
3. Identify information assets and the associated information owners
4. Identify the threats to those assets
5. Identify the vulnerabilities that might be exploited by the threats
6. Identify the impacts that losses of confidentiality, integrity and availability may have on the assets
7. Analyze and evaluate the risks
8. Assess the business impacts on HNE that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of those assets
9. Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented
10. Estimate the level of risks
11. Determine whether the risks are acceptable
12. Identify and evaluate options for the treatment of risk
13. Apply appropriate controls
14. Accept the risks
15. Avoid the risks
16. Mitigate the risks
17. Transfer the associated business risks to other parties
18. Select control objectives and controls for the treatment of risks
19. Document risks in a risk register
20. Track mitigation straggles to closure
21. Reassess annually

~~It is recognized no set of controls will achieve complete security. Additional management action will be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls to support HNE goals and objectives.~~

1. **Information Security Policy and Standard Operating Procedures (SOP) Structure**

To ensure controls are consistently applied to information security functional areas, the following policies:

* ITSEC002PGM Information Security Management Program (This Document)
* ITSEC001POL Security Awareness & Training
* ITSEC002POL Device and Media Controls
* ITSEC003POL Information-Access-Management-Policy (change name to Access Control)
* ITSEC004POL Acceptable Use Policy
* ITSEC005POL Confidentiality of System Security Information
* ITSEC006POL Mobile Device Policy (Roll up into Device and Media Control)
* ITSEC007POL Password Management Policy (Roll up into Access Control)
* ITSEC008POL Asset Management
* ITSEC009POL Protection Against Malicious and Mobile Code
* ITSEC011POL IT Change Management Policy (Move out of InfoSec)
* ITSEC012POL Workstation Security (Change name to End Point Protection)
* ITSEC013POL Incident Response
* ITSEC014POL Technology Equipment Disposal
* ITSEC015POL Local Administrative Privileges
* ITSEC016POL Vulnerability Management
* ITSEC017POL Access Recertification Policy (Roll up into Access Control)
* ITSEC018POL Identification Badge Policy
* ITSEC019POL Multi Factor Authentication
* ITSEC021POL Monitor and Logging
* ITSEC022POL Firewall Policy Management
* ITSEC023POL HNE Open Source Application Security
* ITSEC024POL End of life Unsupported Software and Hardware
* **ITSEC025POL Third-Party Information Security Risk Management (New Policy)**
* **ITSEC026POL Information Security Risk Management (New Policy)**

1. Security Awareness and Training

HNE will implemented a formal, documented security awareness and training program for its workforce members. All workforce members who have access to HNE information systems must understand how to protect the confidentiality, integrity, and availability of the systems. HNE will provide Security Awareness and Training to ensure that all workforce members are equipped with the knowledge and skills necessary to protect the organization's information assets. HNE will foster a culture of security awareness to minimize likelihood of a successful cyber-attack to ensure compliance with regulatory requirements, and promote best practices for safeguarding sensitive information through regular training and updates on the latest security threats and protocols.

HNE provides education and training regarding this Program to all employees who will have access to Personal Information through their employment to HNE

HNE communicates its relevant policies and procedures under this Program to its consultants, interns, and third-party service providers who will have access to Personal Information through their services to HNE

1. **Access Control**

Access to information, information systems, information processing facilities, and business processes will be controlled on the basis of business and security requirements. Formal procedures will be developed and implemented to control access rights to information, information systems, and services to prevent unauthorized access. Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords. Users will be made aware of their responsibilities to ensure unattended equipment has appropriate protection. A clear desk policy for papers and removable storage devices and a clear screen policy will be implemented, especially in work areas accessible by the public. Steps will be taken to restrict access to operating systems to authorized users. Protection will be required commensurate with the risks when using mobile computing and teleworking facilities.

HNE uses secure user authentication protocols, including (i) control of user IDs and other identifiers, (ii) a reasonably secure method of assigning and selecting passwords; and (iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect. HNE assigns unique identification plus passwords that are designed to maintain the integrity of the security of the access controls, and prohibits the use of vendor supplied default passwords, to each authorized active user.

HNE will regularly monitor and verifies electronic access to ensure that such access is limited to authorized users and active user accounts only. This verification process will limit access to records and files containing Personal Health Information and Personal Information to users with a need to access such Personal Health Information and Personal Information in order to perform their job duties. HNE’s Information Security Administrator with input from department managers will determine who shall be an authorized user with an active user account at HNE and which users need such information to perform their job duties.

HNE requires that current computer or network passwords are changed periodically. HNE blocks access to users after multiple unsuccessful attempts to gain electronic access to records or files containing Personal Information.

HNE will block electronic access to Personal Health Information and Personal Information by former employees, other former service providers of HNE, and other individuals who are no longer authorized users with an active user account.

HNE will promptly terminate and prohibit electronic access by former employees, other former service providers of HNE, and other individuals who are no longer authorized users with an active user account to records and files containing Personal Health Information and Personal Information. Voicemail access, email access, HNE internet access, and passwords will be promptly disabled or blocked.

1. **Business Continuity Management**

The objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. A business continuity management process will be established to minimize the impact on Health New England and recover from loss of information assets to an acceptable level through a combination of preventive and recovery controls

1. **Backup and Recovery**

The objective of backup and recovery is to establish and maintain a comprehensive backup and recovery program to ensure the integrity, availability, and confidentiality of its information systems. This program includes conducting regular backups of user-level and system-level information, including system documentation, at frequencies consistent with the organization-defined recovery time and recovery point objectives. Backup data must be stored securely, with cryptographic mechanisms implemented to protect against unauthorized access and modification, and in an immutable format. Backups should be tested regularly to verify media reliability and information integrity, ensuring that system functions can be restored as intended. The organization will also identify alternate storage and processing sites sufficiently separated from the primary sites to reduce susceptibility to the same threats and ensure accessibility during disruptions. Dual authorization is required for the deletion or destruction of backup information to prevent unauthorized actions. Procedures will be documented and regularly updated to adapt to new threats and compliance requirements, ensuring continuous protection and quick recovery from potential data loss events.

1. **Acceptable Use**

Health New England (“HNE”) will create and maintain an Acceptable Use Policy to cover electronic equipment, such as network resources, laptops, cellular phones, portable or removable media (e.g., USB drives), and home computers (collectively, “Equipment”). The equipment may contain sensitive, confidential, or proprietary company data, and/or protected health information (“PHI”), electronic PHI (“ePHI”) and Personal Identifiable (PI), which will be protected as defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (collectively, “Data”). HNE will ensure users who access Equipment will protect the privacy and security of the Equipment and its information at all times, including while outside the physical confines of HNE’s offices. Workforce members will guard HNE equipment against unauthorized access, distribution, disclosure or destruction of Equipment and Data, including PHI, ePHI and PI.

1. Confidentiality of System Security Information
2. Device and Media Controls (Add **mobile device** management here)
3. Password Management (Roll up into Access Control)
4. **Asset Management**

The objective of asset management is to achieve and maintain appropriate protection of Health New England information assets. All assets will be identified. Owners of information assets will be identified and will have responsibility for identifying the classification of those assets and maintenance of appropriate controls. To ensure information receives an appropriate level of protection, information will be classified to indicate the sensitivity and expected degree of protection for handling. Rules for acceptable use of information and information assets will be identified, documented, and implemented.

1. Protection Against Malicious and Mobile Code
2. IT Change Management
3. Workstation Security (Change Name to End Point Protection)

HNE encrypts all Personal Information stored on laptops or other portable devices

1. Incident Response

In accordance with M.G.L. Chapter 93H , Employees, independent contractors, consultants, and interns are required to report any potential security violations, breaches of security, or suspicious or unauthorized use of Personal Information contained in records or files of HNE to the MA Data Privacy Coordinator

Contractors of HNE shall cooperate with HNE when it is the owner or licensor of Personal Information by informing HNE of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the contractor has taken or plans to take relating to the incident (such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use).

HNE documents any responsive actions taken in connection with each security incident. HNE conducts a prompt review of any security incident, including incidents that require notification under the Regulations, and determines whether any changes in this Program are required to improve the security of records and files containing Personal Information.

**Breach Notifications – Massachusetts**

If a “breach of security” has occurred, the MA Data Privacy Coordinator shall provide written notice **as soon as practicable and without unreasonable delay** to:

1. The Attorney General (AGO);
2. The Director of the Office of Consumer Affairs and Business Regulation (OCABR); and
3. The affected Massachusetts resident

Notice Content. (Links to sample letters are included in the attachment section.)

1. The notice to be provided to the AGO and OCABR shall include, but not be limited to:
   1. the nature of the breach of security or unauthorized acquisition or use
   2. the number of residents of the commonwealth affected by such incident at the time of notification
   3. any steps the person or agency has taken or plans to take relating to the incident
2. The notice to be provided to the resident shall include, but not be limited to,
   1. the consumer’s right to obtain a police report
   2. how a consumer requests a security freeze
   3. the necessary information to be provided when requesting the security freeze
   4. any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall **not** include:
      * The nature of the breach or unauthorized acquisition or use or
      * The number of residents of the commonwealth affected by said breach or unauthorized access or use.

**Breach Notifications – HITECH**

1. Technology Equipment Disposal
2. Local Administrative Privileges
3. Vulnerability Management

All operating system security patches on all systems will be maintained for the protection of PHI and PI that are reasonably designed to maintain the integrity of such information

1. Identification Badge Management
2. Multi Factor Authentication
3. **Audit and Log Monitoring (Change policy name)**

The objective of the audit and log monitoring is implement and maintain comprehensive audit and log monitoring procedures to ensure the integrity, confidentiality, and availability of information systems. This includes the generation, review, and analysis of audit records for indications of inappropriate or unusual activity and the potential impact of such activity. The system must be capable of recording event types such as user logins, access to critical data, and configuration changes, among others. Audit records shall be protected against unauthorized access, modification, and deletion. Alerts must be generated in real-time for defined audit logging failures, and measures should be in place to ensure audit log storage capacity is sufficient to avoid loss of logging capability. Automated mechanisms will be used to integrate audit record review with other security processes, facilitating continuous monitoring, incident response, and investigations. The audit and log monitoring processes will be regularly reviewed and updated to address new threats and ensure compliance with applicable regulations and organizational policies.

HNE monitors all computer systems for unauthorized use of or access to records and files containing Personal Information

1. **Firewall Management**

HNE has and will continue to maintain reasonably up-to-date firewall protection

1. **Open Source Application Security**
2. **End of life Unsupported Software and Hardware**
3. **Third-Party Information Security Risk Management**

Vetting Process for Third Party Service Providers. Before engaging a third-party service provider who will have access to Personal Information, HNE conducts reasonable due diligence to assess whether a prospective third-party service provider is capable of safeguarding Personal Information in the manner required by this Program. Due diligence efforts may include, but are not necessarily limited to, discussions with the prospective third-party service provider's personnel, reviewing the prospective third-party service provider's privacy and/or information security policies, and/or requesting the prospective third-party service provider to complete a security questionnaire or otherwise answer security-related questions. HNE may also enter into a contractual agreement with its third-party service providers to protect Personal Information disclosed to such service providers by HNE.

Monitoring. HNE periodically reviews and monitors the performance of its third-party service providers who have access to HNE’s systems and/or Personal Information in order to ensure that each such third-party service provider is applying protective security measures at least as stringent as those required by this Program to be applied to such information.

1. **Information Security Risk Management Program**

HNE will, on a periodic basis, (i) conduct a review to identify reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of any electronic, paper, or other records containing Personal Information; (ii) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Personal Information; (iii) evaluate the sufficiency of this Program to control those risks; and (iv) revise this Program to minimize those risks, consistent with the requirements of the Regulations. This risk assessment will include, but may not be limited to, an assessment of internal and external risks associated with ongoing employee training, employee compliance with this Program, and means for detecting and preventing security system failures.

HNE conducts a formal review of this Program at least annually, and whenever there is a material change in HNE’s business practices that may reasonably implicate the security or integrity of records or files containing Personal Information.

HNE will regularly evaluate its paper, electronic, and other records, electronic systems, and storage media (including laptops and portable devices used to store Personal Information) to determine which records, files, and systems contain Personal Information.

1. **Organization of Information Security**

Information security will be managed within Information Technology (IT), under the direction of the Chief Information Officer (CIO) ~~Vice President of IT~~. Information Security will provide subject matter expertise in security risk assessments, design and deployment of security solutions and technologies. It will lead the creation, implementation and monitoring of appropriate policies, procedures and controls as required by Health New England’s Information Security Management Program. Information Security will also conduct incident response investigations to ensure appropriate reporting and corrective actions are taken. It will conduct workforce training, raise awareness of security threats and best practices and monitor policies, laws and regulations and communicate impacts to Health New England.

1. **Human Resources Security**

All employees, contractors, and third party users of Health New England information and information assets will understand their responsibilities and will be deemed suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse. Security responsibilities will be addressed prior to employment in position descriptions and any associated terms and conditions of employment. Where appropriate, all candidates for employment, volunteer work, contractors, and third party users will be adequately screened, especially for roles that require access to sensitive information. Management is responsible to ensure security is applied through an individual’s employment with Health New England.

All employees, contractors and third party users will receive appropriate awareness training and regular updates on policies and procedures as relevant for their job function.

Procedures will be implemented to ensure an employee’s, contractors, and third party’s exit from Health New England is managed and the return of all equipment and removal of all access rights are completed.

1. **Physical and Environmental Security**

The objective of physical and environment security is to prevent unauthorized physical access, damage, theft, compromise, and interference to Health New England’s information and facilities. Locations housing critical or sensitive information or information assets will be secured with appropriate security barriers and entry controls. They will be physically protected from unauthorized access, damage and interference. Secure areas will be protected by appropriate security entry controls to ensure that only authorized personnel are allowed access. Security will be applied to off-site equipment. All equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal in compliance with company policies.

Physical Security of PHI or PI

1. **Use and Storage of Files:** Employees, consultants, and interns of HNE must follow ~~HNE’s Privacy and Security~~ Policy requirements regarding documents or files containing Personal Information on their desks when they are not at their desks or in any other unsecured, unattended place. This policy applies to both hard-copies and electronic copies of records and files containing Personal Information. At the end of the work day, all files and other records containing Personal Information must be secured in a manner that is consistent with this Program and the requirements of the Regulations.
2. Blocked Physical Access. HNE prohibits and blocks physical access to records and files containing Personal Information by any individual without authorization to access such records. HNE is a locked facility and requires the use of security badges for entrance to its premises. Employees, consultants, and interns of HNE are required, upon termination or resignation for any reason, or earlier if upon the request of HNE, to surrender all keys, IDs, access codes, badges, business cards, and the like, that permit access to HNE’s premises or to records of HNE containing Personal Information.
3. Visitors. All visitors to HNE must be registered at the visitor’s entrance on the 15th Floor and must be accompanied by an approved employee. Visitors of HNE are prohibited and blocked from accessing any records or files of HNE containing Personal Information.
4. **Information Management**

Personal Information must be created, stored, disclosed, transmitted, and disposed of in the following manner:

1. **Creation**: Upon creation of paper and/or electronic documents and files that contain Personal Health Information (PHI) or Personal Information (PI), such documents and files must be identified and treated as "Confidential”.
2. **Storage**: Paper documents containing PHI or PI ~~Personal Information~~ must be stored in a locked or otherwise secured desk, file cabinet, office, or controlled area when unattended. Storage of electronic PHI or PI ~~Personal Information~~ should be kept to a minimum. Any questions regarding HNE’s encryption technology should be directed to the HNE’s Chief Information Security Officer.
3. **Transmission**: Voice communications involving PHI or PI ~~Personal Information~~ must be kept to a minimum and performed in closed or secured locations. Transmission of PHI or PI ~~Personal Information~~ in paper or hard-copy form outside of HNE, or other removal of PHI or PI ~~Personal Information~~ from HNE’s premises, must be done with reasonable precaution and in accordance with any applicable HNE procedures and/or rules to ensure the security of such information and to prevent unauthorized disclosure. Transmission of electronic PHI or PI ~~Personal Information~~ must be encrypted, and must likewise be done with reasonable precaution to ensure the security of such information and to prevent unauthorized disclosure.
4. **Disposal**: PHI or PI ~~Personal Information~~ must be disposed of when no longer required by HNE for immediate use or for a specific business purpose. Where appropriate, paper documents and other hard-copies of records or files containing PHI or PI ~~Personal Information~~, determined by HNE to be no longer required, should be disposed of by cross-cut shredding, incineration, pulping, redaction, or burning, so that such PHI or PI ~~Personal Information~~ cannot practicably be read or reconstructed. PHI or PI ~~Personal Information~~ determined by HNE to be no longer required must be destroyed or erased so that such PHI or PI ~~Personal Information~~ cannot practicably be read or reconstructed.
5. **Communications and Operations Management**

Responsibilities and procedures for the management and operation of all information processing facilities will be established. As a matter of policy, segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system or information misuse. Precautions will be used to prevent and detect the introduction of malicious code and unauthorized mobile code to protect the integrity of software and information. To prevent unauthorized disclosure, modification, removal or destruction of information assets, and interruption to business activities, media will be controlled and physically protected. Procedures for handling and storing information will be established and communicated to protect information from unauthorized disclosure or misuse. Exchange of sensitive information and software with other organizations will be based on a formal exchange policy. Media containing information will be protected against unauthorized access, misuse or corruption during transportation beyond Health New England’s physical boundaries.

To detect unauthorized access to Health New England’s information and information systems, systems will be monitored and information security events will be recorded. Health New England will employ monitoring techniques to comply with applicable company policies related to acceptable use

1. **Information Systems Acquisition, Development and Maintenance**

Policies and procedures will be employed to ensure the security of information systems. Encryption will be used, where appropriate, to protect sensitive information at rest and in transit. Access to system files and program source code will be controlled and information technology projects and support activities conducted in a secure manner. Technical vulnerability management will be implemented with measurements taken to confirm effectiveness. It may be necessary, from time to time, to store HNE data in applications or databases hosted off HNE premises. In order to manage and control the risk inherent in that, data will only be entrusted to vendors who can demonstrate appropriate controls and security measures sufficient to ensure the safety of that data. Any data not stored on HNE premises must be located in the United States (onshore) to ensure regulatory and legal accountability and jurisdiction. Exceptions to the policy (data located offshore) must be evaluated for risk and approved by the IT Executive Risk Management committee.

1. **Information Security Incident Management**

Information security incidents will be communicated in a manner allowing timely corrective action to be taken. Formal incident reporting and escalation procedures will be established and communicated to all users. Responsibilities and procedures will be established to handle information security incidents once they have been reported

1. **~~Compliance~~**

~~The design, operation, use, and management of information and information assets are subject to statutory, regulatory, and contractual security requirements. Compliance with legal requirements is necessary to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. Legal requirements include, but are not limited to: state statute, statewide and agency policy, regulations, contractual agreements, intellectual property rights, copyrights, and protection and privacy of personal information.~~

~~Controls will be established to maximize the effectiveness of the information systems audit process. During the audit process, controls will safeguard operational systems and tools to protect the integrity of the information and prevent misuse.~~

1. **Configuration Management**

Configuration management ensures the integrity and security of its information systems. This program includes developing, documenting, and implementing configuration management policies and procedures that address roles, responsibilities, and processes throughout the system development life cycle. A baseline configuration for each system, or system group, must be developed and maintained, reflecting all system components, configurations, and operational details. All changes to system configurations must be reviewed, approved, documented, and tested for security and privacy impacts before implementation. Automated mechanisms will be used to manage, apply, and verify configuration settings, ensuring accuracy and compliance with organizational policies. Configuration items under management include software, hardware, firmware, and documentation. The Configuration Management program must also include provisions for the retention of previous configurations to support rollback and the implementation of automated tools to detect and respond to unauthorized changes.

1. **System and Information Integrity**

This program includes the deployment of automated tools for integrity verification, real-time monitoring, and notification of integrity violations. It encompasses controls for flaw remediation, malicious code protection, security alerts, and error handling. The integrity of software, firmware, and information is ensured through cryptographic mechanisms, integrity verification at system startup, and continuous monitoring for unauthorized changes. Cryptographic functions include encryption of all records and files containing PHI and PI transmitted across public networks or wirelessly. Additionally, the organization will integrate detection and response capabilities into its incident response processes to promptly address integrity violations. Procedures will be established to manage system configurations, apply necessary updates, and verify system and information integrity regularly. The policy and associated procedures will be reviewed and updated periodically to adapt to new threats and ensure compliance with applicable regulations and organizational standards.

1. **Roles and Responsibilities**

**MA Data Privacy Coordinator:** TheHNE’s Chief Compliance Officer will be responsible, with the support of:

1. Develop, implement, administer, monitor, review, and update this Privacy Program from time to time, consistent with the requirements of the Regulations;
2. Oversee ongoing employee training, including temporary and contract employees, and any communications involving this Program;
3. With HNE’s Information and Security Officer, address any information security issues, including employee compliance and access to HNE’s personal information by former employees, that may arise from time to time, and provide input to HNE’s Human Resource Department regarding the imposition of disciplinary measures for violations of the Program; and
4. Take all reasonable steps to verify that any third-party service provider with access to HNE’s personal information has the capacity to protect such personal information in the manner consistent with this Program and the requirements of the Regulations and that any such third-party service provider applies protective security measures at least as stringent As those required by the Regulations.

Chief Information Officers:

Chief Information Security Officer:

Information Security Analyst

Director of Infrastructure

**Definitions**

* **Immutable Backups**: Unable to be changed. This ensures that ransomware cannot be written to the backups
* **Personal Health Information**: refers to any information that is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse and relates to an individual's past, present, or future physical or mental health condition, the provision of healthcare, or payment for healthcare. It includes any information that can be used to identify (18 Identifiers) the individual, such as demographic data, medical history, test results, insurance information, and other details concerning a patient's care. PHI can be in any form or medium, including electronic, paper, or oral formats.
* **18 PHI (Protected Health Information) identifiers**: defined by HIPAA include names; geographic subdivisions smaller than a state, such as street address, city, county, precinct, and zip code, except for the initial three digits of a zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; all elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, and date of death, and all ages over 89 and all elements indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; telephone numbers; fax numbers; email addresses; Social Security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web URLs; Internet Protocol (IP) addresses; biometric identifiers, including finger and voice prints; full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code.
* **Personal Information, as per The Commonwealth of Massachusetts Privacy Law**: "Personal Information" means a Massachusetts resident's first name and last name, or first initial and last name, in combination with anyone or more of the following data elements that relate to such resident: (a) social Security number, (b) driver's license number or state-issued identification card number, or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account. "Personal Information" does not, however, include Information that is lawfully obtained from publicly available Information, or from federal, state, or local government records lawfully made available to the general public.
* **Breach of security**: means the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.
* **PHI**: Personal Health Information
* **PI**: Personal Information

**References**

164.308(a)(1-4), 164.308(a)(6-7)

**Signatures**

All signature, Policy Owner Review, Additional Reviewer, and Final Approval, are captured electronically.