Secure Health Information Technology Corp.

SECURITY PRIVACY and CONFIDENTIALITY PLAN

Index

This security plan describes SecureHIT's safeguards to protect confidential information belonging to patients in accordance with the Health Insurance Portability Accountability Act, SecureHIT implements the following policies and procedural safeguards to insure the security and privacy of confidential information.

Scope of Confidential Information Covered

Health Insurance Portability Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) requires SecureHIT to adhere to policies regarding private health information. HIPAA requires SecureHIT to maintain the privacy of your Protected Health Information (ePHI). We protect your ePHI from inappropriate use or disclosure. Our employees, and those companies that help us service patients and employees, are required to comply with our requirements that protect the confidentiality of ePHI. They may look at ePHI only when there is an appropriate and valid reason to do so. We will not disclose ePHI to any other company for their use in marketing their products.

This Information Security Plan provides mechanisms to:

Ensure the security and confidentiality of covered data and information;
Protect against anticipated threats or hazards to the security or integrity of such information;
Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any patience;
Identify and assess the risks that may threaten covered data and information maintained by SecureHIT;
Train employees on maintaining the privacy of covered ePHI data;
Implement and review the plan; and
Adjust the plan to reflect changes in technology, the sensitivity of covered ePHI data, information and internal or external threats to information security.

Identification and Assessment of Risks to Confidential Information

SecureHIT recognizes that it has both internal and external risks to the security of information covered under this policy. These risks include, but are not limited to:

Unauthorized access to covered data and information and educational records by someone other than the owner of the covered data and information;
Compromised system security as a result of system access by unauthorized persons;
Interception of data during transmission;
Loss of data integrity;
Physical loss of data in a disaster;
Errors introduced into the system;

Corruption of data or systems;
Unauthorized access of covered data and information by employees;
Unauthorized requests for covered ePHI data and information;
and Unauthorized transfer of covered data and information through third parties.

SecureHIT recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Chief Information Security Officer, in consultation with the Chief Executive Officer, will actively monitor advisory groups such as the NIST, CISA, FTC, SBA, DHS for identification of new risks.

SecureHIT believes that ITs current safeguards are reasonable and, in light of current risk assessments and SecureHIT's compliance with procedural safeguards under the laws covered under this policy and any applicable state privacy laws, are sufficient to provide security and confidentiality to covered data and information maintained by SecureHIT. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

Design and Implementation of Safeguards Program:

Security Plan Coordinators

The CEO, in consultation with the Information Systems Security Officer, will serve as the coordinator of this Plan. Together, they will assess the risks associated with unauthorized transfers of covered ePHI data and implement procedures to minimize those risks.

Employee Management and Training

SecureHIT checks references of new employees working in areas that regularly work with covered ePHI data.

During employee orientation, each new employee in these departments will receive proper training on the importance of confidentiality of patient's records, student and other types of covered ePHI data and information. Each new employee is also/will also be trained in the proper use of computer information and passwords. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including how to properly dispose of documents that contain covered ePHI data and information. Each department responsible for maintaining covered ePHI data and information will be instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. These training efforts should help minimize risk and safeguard covered ePHI data and information security.

Physical Security

SecureHIT has addressed the physical security of the information with AWS Certifications.

Information Systems

Access to covered ePHI data via the information system is limited to those employees who have a legitimate reason. Each employee is assigned a username and password. Databases containing patients covered ePHI data, are available only to SecureHIT employees in appropriate positions.

Services such as Direct Messaging are protected by requiring a valid and verified user to provide a valid user username, password and MFA. If a user does not have a valid combination, they are not given access.

● Definitions:

ISO - Information Systems Officer.

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: SecureHIT HIE

1.1.1. System Categorization: Moderate Impact for Confidentiality

1.1.2. System Unique Identifier: SecureHIT

1.2. Responsible Organization:

Name:	Janet Rios
Address:	California st #25 Casablanca Toa Alta, PR 00953
Phone:	787-562-7036

1.2.1. Information Owner:

Name:	Janet Rios
Title:	CEO
Office Address:	#25 California st Casablanca Toa Alta, PR 00953
Work Phone:	787-562-7036
e-Mail Address:	jrios@securehitpr.com

1.2.1.1.System Owner (assignment of security responsibility)**:**

Name:	Samuel Rivera
Title:	Information Systems Administrator
Office Address:	Opalo st P16 urb Madelaine Toa Alta, PR 00953
Work Phone:	787-234-4330
e-Mail Address:	srivera@securehitpr.com

1.2.1.2. System Security Officer:

Name:	Jose A Miranda
ISSTitle:	ISSO
Office Address:	1129 Italia st
Work Phone:	7875533354
e-Mail Address:	jmiranda@securehitpr.com

1.3.General Description/Purpose of System: What is the function/purpose of the system?

Health Information Service Provider, HIE, EHR, Exchange Direct Secure Messages, FHIR exchange.

1.3.1. Number of end users and privileged users: **4**

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users
5	2

1.4.General Description of Information:

SecureHIT HIE Sends and Received Secure Direct Secure Messages, FHIR from EHRs, HIE's and another HISPs

2. SYSTEM ENVIRONMENT

SecureHIT servers are in a Virtual Private Cloud in Amazon Web Services AWS, both have share responsibility with AWS been responsible for Physical security, cooling, power, Physical redundancy while SecureHIT is responsible of the virtual security, access, information backups, etc, using linux servers, VPN server, firewalls, routers, switches.

2.1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

EC2 AWS Linux servers
AWS RDS Services
OpenVPN Server
The ISO is the person responsible.

2.2. List all software components installed on the system.

AWS Linux, RDS MySQL, DirectTrust Java reference Implementation, Apache Tomcat, Apache WebServer, Apache James, OpenVPN Server, SecureHIT API.

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization?

No, Physical and virtual Machines are property of AWS.

AWS Automatic security updates.

3. REQUIREMENTS

(Note: The source of the requirements is NIST Special Publication 800-53)

SecureHIT utilices Certificates, and a Direct Trust Certificate Bundle that provides a Secure environment to transmite Direct Secure Messages, FHIR and other secure protocols.

HIPAA federal and local Laws requirements
Certifications from EHNAC and DirectTrust.
Vetting of all System users.
Penetration testing by third party security.
MFA for user access to portals
User, password, certificate with Encrypted tunnel for access to data center.
Security Information Event Management (Siem).
Audit plan and controls.
Antivirus for equipment to access data center.
Plans and processes for exercising and maintaining plans are schedule on the ServiceDesk.
Annual update process for this Plan schedule on the ServiceDesk.
Data breach reporting processes are stated on policies and procedures.
Cybersecurity Awareness program schedule on ServiceDesk.
Entitlement Reviews schedule on ServiceDesk.

EHNAC - DirectTrust Privacy & Security: This program accredits organizations against our core criteria. These criteria address not only privacy and security, but customer service, business practices, personnel requirements, third-party cloud service providers, and more. This program is applicable for organizations with stakeholder-specific services that are not addressed by any of our other programs.

3.1.Access Control

3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Token, MFA, OpenVPN Authentication limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

3.1.2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Token, MFA, OpenVPN Authentication limit system access to the types of transactions and functions that authorized users are permitted to execute.

3.1.3. Control the flow of CUI in accordance with approved authorizations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Token, MFA, OpenVPN Authentication control the flow of CUI in accordance with approved authorizations.

3.1.4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Duties has been separted for all employees and clients. separate the duties of individuals to reduce the risk of malevolent activity without collusion.

3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
The principle of least privilege has been implemented. employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6. Use non-privileged accounts or roles when accessing nonsecurity functions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
The principle of least privilege has been implemented. use non-privileged accounts or roles when accessing nonsecurity functions.

3.1.7. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
The principle of least privilege has been implemented. prevent non-privileged users from executing privileged functions and audit the execution of such functions.

3.1.8. Limit unsuccessful login attempts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Configure all environments to Limit unsuccessful logon attempts.

3.1.9. Provide privacy and security notices consistent with applicable CUI rules.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Provide privacy and security notices consistent with applicable CUI rules.

3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity

3.1.11. Terminate (automatically) a user session after a defined condition.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Terminate (automatically) a user session after a defined condition.

3.1.12. Monitor and control remote access sessions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Monitor and control remote access sessions.

3.1.13. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

3.1.14. Route remote access via managed access control points.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
3.1.15. Route remote access via managed access control points.

3.1.16. Authorize remote execution of privileged commands and remote access to security-relevant information.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
3.1.17. Authorize remote execution of privileged commands and remote access to security-relevant information.

3.1.18. Authorize wireless access prior to allowing such connections.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
3.1.19. Authorize wireless access prior to allowing such connections.

3.1.20. Protect wireless access using authentication and encryption.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
3.1.21. Protect wireless access using authentication and encryption.

3.1.22. Control connection of mobile devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Control connection of mobile devices.

3.1.23. Encrypt CUI on mobile devices and mobile computing platforms.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
3.1.24. Encrypt CUI on mobile devices and mobile computing platforms.

3.1.25. Verify and control/limit connections to and use of external systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
3.1.26. Verify and control/limit connections to and use of external systems.

3.1.27. Limit use of organizational portable storage devices on external systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
NO use of organizational portable storage devices on external systems.

3.1.28. Control CUI posted or processed on publicly accessible systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
NO CUI posted or processed on publicly accessible systems.

3.2.Awareness and Training

3.2.1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT ensures that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

3.2.2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT ensures that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

3.2.3. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SecureHIT provides security awareness training on recognizing and reporting potential indicators of insider threat.

3.3.Audit and Accountability

3.3.1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT retains system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

3.3.2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT ensures that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

3.3.3. Review and update logged events.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT Review and update logged events.

3.3.4. Alert in the event of an audit logging process failure.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT alerts in the event of an audit logging process failure.

3.3.5. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

3.3.6. Provide audit record reduction and report generation to support on-demand analysis and reporting.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT provide audit record reduction and report generation to support on-demand analysis and reporting.

3.3.7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

3.3.8. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT protect audit information and audit logging tools from unauthorized access, modification, and deletion.

3.3.9. Limit management of audit logging functionality to a subset of privileged users.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT limit management of audit logging functionality to a subset of privileged users.

3.4.Configuration Management

3.4.1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

☒ Implemented ☐ Planned to be Implemented ☒ Not Applicable
SecureHIT establish and maintain baseline configurations and inventories of organizational systems.

3.4.2. Establish and enforce security configuration settings for information technology products employed in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☒ Not Applicable
SecureHIT establish and enforce security configuration settings for information technology products employed in organizational systems.

3.4.3. Track, review, approve or disapprove, and log changes to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT track, review, approve or disapprove, and log changes to organizational systems.

3.4.4. Analyze the security impact of changes prior to implementation.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT analyze the security impact of changes prior to implementation.

3.4.5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

3.4.6. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

3.4.7. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

☒ Implemented ☐ Planned to be Implemented ☒ Not Applicable
SecureHIT restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

3.4.8. Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

3.4.9. Control and monitor user-installed software.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT control and monitor user-installed software.

3.5.Identification and Authentication

3.5.1. Identify system users, processes acting on behalf of users, and devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT identify system users, processes acting on behalf of users, and devices.

3.5.2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

3.5.4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

3.5.5. Prevent reuse of identifiers for a defined period.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT prevent reuse of identifiers for a defined period.

3.5.6. Disable identifiers after a defined period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT disable identifiers after a defined period of inactivity.

3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT enforce a minimum password complexity and change of characters when new passwords are created.

3.5.8. Prohibit password reuse for a specified number of generations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT Prohibit password reuse for a specified number of generations.

3.5.9. Allow temporary password use for system logons with an immediate change to a permanent password.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT allow temporary password use for system logons with an immediate change to a permanent password.

3.5.10. Store and transmit only cryptographically-protected passwords.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT store and transmit only cryptographically-protected passwords.

3.5.11. Obscure feedback of authentication information.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT obscure feedback of authentication information.

3.6.Incident Response

3.6.1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

3.6.2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

3.6.3. Test the organizational incident response capability

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT test the organizational incident response capability.

3.7.Maintenance

3.7.1. Perform maintenance on organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT performs maintenance on organizational systems.

3.7.2. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

3.7.3. Ensure equipment removed for off-site maintenance is sanitized of any CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT ensure equipment removed for off-site maintenance is sanitized of any CUI.

3.7.4. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT checks media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

3.7.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

3.7.6. Supervise the maintenance activities of maintenance personnel without required access authorization.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT supervise the maintenance activities of maintenance personnel without required access authorization.

3.8.Media Protection

3.8.1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SecureHIT protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

3.8.2. Limit access to CUI on system media to authorized users.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT limit access to CUI on system media to authorized users.

3.8.3. Sanitize or destroy system media containing CUI before disposal or release for reuse.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT sanitize or destroy system media containing CUI before disposal or release for reuse.

3.8.4. Mark media with necessary CUI markings and distribution limitations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT mark media with necessary CUI markings and distribution limitations.

3.8.5. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

3.8.6. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

3.8.7. Control the use of removable media on system components.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT control the use of removable media on system components.

3.8.8. Prohibit the use of portable storage devices when such devices have no identifiable owner.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT prohibit the use of portable storage devices when such devices have no identifiable owner.

3.8.9. Protect the confidentiality of backup CUI at storage locations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT protect the confidentiality of backup CUI at storage locations.

3.9.Personnel Security

3.9.1. Screen individuals prior to authorizing access to organizational systems containing CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT screen individuals prior to authorizing access to organizational systems containing CUI.

3.9.2. Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

3.10. Physical Protection

3.10.1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

3.10.2. Protect and monitor the physical facility and support infrastructure for organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT protect and monitor the physical facility and support infrastructure for organizational systems.

3.10.3. Escort visitors and monitor visitor activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT escort visitors and monitor visitor activity.

3.10.4. Maintain audit logs of physical access.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT maintain audit logs of physical access.

3.10.5. Control and manage physical access devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT control and manage physical access devices.

3.10.6. Enforce safeguarding measures for CUI at alternate work sites.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT enforce safeguarding measures for CUI at alternate work sites.

3.11. Risk Assessment

3.11.1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

3.11.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

3.11.3. Remediate vulnerabilities in accordance with risk assessments.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT remediate vulnerabilities in accordance with risk assessments.

3.12. Security Assessment

3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SecureHIT periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

3.12.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SecureHIT develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SecureHIT monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.12.4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SecureHIT develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

3.13. System and Communications Protection

3.13.1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SecureHIT monitors, controls, and protects communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SecureHIT eEmploy architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

3.13.3. Separate user functionality from system management functionality.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT separates user functionality from system management functionality.

3.13.4. Prevent unauthorized and unintended information transfer via shared system resources.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT prevents unauthorized and unintended information transfer via shared system resources.

3.13.5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT implements subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

3.13.6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

3.13.7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT prevents remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT implements cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

3.13.9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT terminates network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

3.13.10. Establish and manage cryptographic keys for cryptography employed in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT establishes and manages cryptographic keys for cryptography employed in organizational systems.

3.13.11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT employs FIPS-validated cryptography when used to protect the confidentiality of CUI.

3.13.12. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT prohibits remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

3.13.13. Control and monitor the use of mobile code.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT control and monitor the use of mobile code.

3.13.14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

3.13.15. Protect the authenticity of communications sessions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT protects the authenticity of communications sessions.

3.13.16. Protect the confidentiality of CUI at rest.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

SecureHIT protects the confidentiality of CUI at rest.

3.14. System and Information Integrity

3.14.1. Identify, report, and correct system flaws in a timely manner.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT identifies, report, and correct system flaws in a timely manner.

3.14.2. Provide protection from malicious code at designated locations within organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT provides protection from malicious code at designated locations within organizational systems.

3.14.3. Monitor system security alerts and advisories and take action in response.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT monitors system security alerts and advisories and takes action in response.

3.14.4. Update malicious code protection mechanisms when new releases are available.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT updates malicious code protection mechanisms when new releases are available.

3.14.5. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT performs periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

3.14.6. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT monitors organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

3.14.7. Identify unauthorized use of organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
SecureHIT identifies unauthorized use of organizational systems.

4. RECORD OF CHANGES

Date	Description	Made By:
07/31/2020	Created	JAM
07/31/2021	Review	JAM
07/31/2022	Review	JAM
01/31/2023	Review	JAM
01/31/2024	Review	JAM

Acreditations:

EHNAC (Electronic Healthcare Network Accreditation Commission) is the premier accreditation authority promoting standards that support interoperability, stakeholder trust, regulatory compliance, quality service, innovation, and open competition within the healthcare industry. EHNAC promotes accreditation in the healthcare industry to achieve quality and trust in healthcare information exchange through adoption and implementation of standards.

Secure Exchange Solutions, Inc. has successfully completed the accreditation process of EHNAC by providing evidence that meets the EHNAC criteria in the following areas:

- Identification of data flows of confidential information such as Protected Health Information within the organization as well as with business partners outside of the organization;
- Verification that appropriate Business Associate Agreements are in place with all relevant entities;

- Review of HIPAA privacy policies and procedures;
- Review of HIPAA security safeguards in place (administrative, technical and physical);
- Review methods of secure transmission of data;
- Review of customer service metrics;
- Validation of accuracy of transaction exchange;
- Validation of system availability and capacity metrics;
- Validation of compliance with industry standards;
- Review of IT security best practices;
- Review of industry-specific best practices;
- Review of disaster recovery and business continuity processes;
- Review of workforce training; and
- Review of personnel qualifications.

This Certificate of Accreditation was issued by EHNAC after an objective and independent audit and review of all facilities in-scope of the accreditation, including datacenters and outsourced business partners. Secure Health Information Technology Corp. has been accredited under the EHNAC HISP Privacy and Security Program and Cloud Enabled Accreditation Program.

Security Plan for Confidential Information

This security plan describes SecureHIT's safeguards to protect confidential information belonging to students, staff, alumni, donors and to visitors and users of its websites and servers. In accordance with the Health Insurance Portability Accountability Act, SecureHIT implements the following policies and procedural safeguards to insure the security and privacy of confidential information.

Scope of Confidential Information Covered

Health Insurance Portability Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) requires SecureHIT to adhere to policies regarding private health information. HIPAA requires SecureHIT to maintain the privacy of your Protected Health Information (ePHI). We protect your ePHI from inappropriate use or disclosure. Our employees, and those companies that help us service patients and employees, are required to comply with our requirements that protect the confidentiality of ePHI. They may look at ePHI only when there is an appropriate and valid reason to do so. We will not disclose ePHI to any other company for their use in marketing their products.

This Information Security Plan provides mechanisms to:

Ensure the security and confidentiality of covered data and information;

Protect against anticipated threats or hazards to the security or integrity of such information;

Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any patience;

Identify and assess the risks that may threaten covered data and information maintained by SecureHIT;

Train employees on maintaining the privacy of covered ePHI data;

Implement and review the plan; and Adjust the plan to reflect changes in technology, the sensitivity of covered ePHI data, information and internal or external threats to information security.

Identification and Assessment of Risks to Confidential Information

SecureHIT recognizes that it has both internal and external risks to the security of information covered under this policy. These risks include, but are not limited to:

Unauthorized access to covered data and information and educational records by someone other than the owner of the covered data and information;

Compromised system security as a result of system access by unauthorized persons;

Interception of data during transmission;

Loss of data integrity;

Physical loss of data in a disaster;

Errors introduced into the system;

Corruption of data or systems;

Unauthorized access of covered data and information by employees;

Unauthorized requests for covered ePHI data and information;

and Unauthorized transfer of covered data and information through third parties.

SecureHIT recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Chief Information Security Officer, in consultation with Chief Executive Officer will actively monitor advisory groups such as the NIST, CISA, FTC, SBA, DHS for identification of new risks.

SecureHIT believes that IT's current safeguards are reasonable and, in light of current risk assessments and SecureHIT's compliance with procedural safeguards under the laws covered under this policy and any applicable state privacy laws, are sufficient to provide security and confidentiality to covered data and information maintained by SecureHIT. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

Design and Implementation of Safeguards Program:

Security Plan Coordinators

The CEO, in consultation with the Information Systems Security Officer, will serve as the coordinator of this Plan. Together, they will assess the risks associated with unauthorized transfers of covered ePHI data and implement procedures to minimize those risks.

Employee Management and Training

SecureHIT checks references of new employees working in areas that regularly work with covered ePHI data.

During employee orientation, each new employee in these departments will receive proper training on the importance of confidentiality of patients records, student and other types of covered ePHI data and information. Each new employee is also/will also be trained in the proper use of computer information and passwords. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including how to properly dispose of documents that contain covered ePHI data and information. Each department responsible for maintaining covered ePHI data and information will be instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. These training efforts should help minimize risk and safeguard covered ePHI data and information security.

Physical Security

SecureHIT has addressed the physical security the information with AWS Certifications.

Information Systems

Access to covered ePHI data via the information system is limited to those employees who have a legitimate reason. Each employee is assigned a user name and password. Databases containing patients covered ePHI data, are available only to SecureHIT employees in appropriate positions.

Services such as Direct Messaging are protected by requiring a valid and verified user to provide a valid user username, password and MFA. If a user does not have a valid combination, they are not given access.

Encryption technology is used and utilized for both storage and transmission. All covered ePHI data and information will be maintained on servers that are behind the AWS several firewalls. All firewall software and hardware maintained by AWS will be kept current as per agreement.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that the SecureHIT determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data and

information, the evaluation process shall include the ability of the service provider to safeguard ePHI information. Contracts with service providers will include one or more the following provisions:

An explicit acknowledgment that the contract allows the contract partner access to confidential information;

A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;

An assurance from the contract partner that the partner will protect the confidential information it receives according to HIPAA standards and no less rigorously than it protects its own confidential information;

A provision for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;

An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles the SecureHIT to terminate the contract without penalty; and

A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Notification of Security Incidents

SecureHIT shall notify the owner of ePHI and agencies required by law of any breach of the security of covered ePHI data and information immediately following discovery, if the information, was, or is reasonably believed to have been, acquired by an unauthorized person.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the CEO and ISSO who will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology or law, the sensitivity of patient ePHI data and internal or external threats to information security.

Collaboration Index at: **SecureHIT_Security_and_Privacy_Control_Collaboration_Index.docx**

Janet Ríos Colón

Digitally signed by Janet Ríos Colón
Date: 2024.03.13 12:40:56 -04'00'