etHIN East Tennessee Health Information Network	**SUBJECT:** etHIN Health Information Privacy and Security Policies
	GENERATED BY: etHIN Legal
	APPROVED BY: etHIN Board Operations Committee 4/16/2021
ISSUED: 12/17/2011	**REVISED:** 07/30/2019; 4/16/2021

SCOPE

etHIN operations

PURPOSE

To describe etHIN's overall compliance with applicable statutes and regulations relating to the privacy and security of health information, including but not limited to the Privacy and Security Standards of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA Privacy and Security Standards"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the 21st Century Cures Act ("Cures Act").

POLICY

As a "business associate" within the meaning of HIPAA's Privacy and Security Standards, etHIN complies with HIPAA business associate agreements and applicable law in ensuring the confidentiality and security of Protected Health Information.

As a "health information exchange" within the meaning of the Cures Act, etHIN complies with all applicable provisions of the Cures Act and any applicable regulations issued pursuant thereto relating to the availability and use of electronic health information.

I. <u>PRIVACY POLICIES</u>

A. HIPAA BUSINESS ASSOCIATE. etHIN is a "business associate" relative to Participating Providers and enters into HIPAA business associate agreements with Participating Providers consistent with applicable law. etHIN and its workforce comply with all applicable federal and state laws and regulations related to the use, disclosure and protection of Protected Health Information.

B. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION. etHIN uses and discloses Protected Health Information to perform functions, activities, or services for, or on behalf of, Participating Providers consistent with etHIN's agreements with such Participating Providers, including uses and disclosures necessary to facilitate access to electronic health records (including availability and use of electronic health information pursuant to the Cures Act) and for purposes of Treatment, coordination of care and case management, Payment, public health reporting, relaying information regarding decedents, organ donation and transplantation, and emergencies. etHIN also uses Protected Health Information for its proper management and administration and to carry out its legal responsibilities. etHIN discloses Protected Health Information for the proper management and administration of etHIN or to carry out etHIN's legal responsibilities, provided that such disclosures are Required by Law, or etHIN obtains reasonable assurances (including any legally required assurances) from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies etHIN of any instances of which it is aware in which the confidentiality of the information has been breached. If etHIN provides Data Aggregation services to a Participating Provider, etHIN uses Protected Health Information to provide such Data Aggregation services as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B). etHIN to the extent practicable, limits uses, disclosures, and requests for Protected Health Information to a Limited Data Set (as defined in 45 C.F.R. § 164.514(e)(2)) or to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request (as described in 45 C.F.R. § 164.502(b)(1) and in any guidance issued by the Secretary of the Department of Health and Human Services). etHIN does not use or disclose Protected Health Information other than as permitted or required by these policies, any applicable business associate agreement, or as Required by Law.

C. SAFEGUARDS AGAINST MISUSE OF INFORMATION AND MITIGATION. etHIN implements and uses appropriate safeguards to prevent the use or disclosure of Protected Health Information other than in accordance with these policies and its business associate agreements. Such safeguards include training its workforce on the key requirements of the Privacy and Security Standards prior to access to any Protected Health Information and periodically thereafter, with documentation of such training maintained for etHIN's files. etHIN mitigates, to the extent practicable, harmful effects known to etHIN of a use or disclosure in violation of the requirements of its policies and business associate agreements (e.g., by recovering inappropriately disclosed Protected Health Information or ensuring its destruction).

> **1. E-Mail Encryption.** E-mail communications containing Protected Health Information (e.g., name, address, social security number, date of birth or any other information that may be used alone or in combination with other information to identify a patient) and sent outside the etHIN network shall be sent via secure encrypted means or shall be de-identified. E-mail communications shall include a privacy statement informing recipients that the information is confidential and to alert the sender if a message is received in error.
>
> **2. Fax.** Before faxing any Protected Health Information, etHIN employees shall verify the name of the recipient and the fax number. A cover sheet with a privacy statement and the sender's name and phone number shall be used for all faxed communications.

D. REPORTING OF USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION. etHIN workforce members must immediately report any suspected inappropriate access, use, or disclosure of Protected Health Information or potential breach in the privacy or security of such information (e.g., information sent to incorrect recipient) to etHIN's Privacy Officer. After appropriate internal investigation, by etHIN's Privacy Officer, etHIN reports to applicable Participating Providers known uses or disclosures of Protected Health Information in violation of a business associate agreement by etHIN, its officers, directors, employees, contractors, or agents, or by a third party to which etHIN disclosed Protected Health Information. etHIN's Privacy Officer ensures that etHIN's Board of Directors and Operations Council is apprised of inappropriate access, use, or disclosure of Protected Health Information or breach in the privacy or security of such information.

E. AGREEMENTS WITH THIRD PARTIES. To the extent required by law, etHIN enters into agreements with third parties that etHIN provides with Protected Health Information requiring such third parties to comply with the restrictions, terms, and conditions that apply to etHIN under business associate agreements with Participating Providers.

F. ACCESS. To the extent etHIN holds Protected Health Information in a Designated Record Set, etHIN makes such information available consistent with the requirements of 45 C.F.R. § 164.524.

G. COMMUNICATED RESTRICTIONS. etHIN complies with communicated restrictions in the use or disclosure of Protected Health Information to which Participating providers have agreed, and to the extent communicated by a Participating Provider, complies with any Individual's request for restrictions on Protected Health Information disclosures that a Participating Provider or etHIN is required by law to honor, including requested restrictions on Payment or Health Care Operations-related disclosures to Health Plans when the Individual's involved Health Care Provider has been paid out of pocket in full.

H. ACCOUNTING FOR USES AND DISCLOSURES. etHIN documents and makes available to Participating Providers information regarding uses and disclosures of Protected Health Information as are required for the Participating Provider to respond to a request by an Individual for an access report or an accounting of disclosures of Protected Health Information consistent with the requirements of applicable law.

I. AMENDMENTS TO PROTECTED HEALTH INFORMATION/RECORDS. etHIN makes amendments to Protected Health Information in any Designated Record Sets held by etHIN that a Participating Provider directs or agrees to pursuant to 45 C.F.R. § 164.526, at the request of the Participating Provider or an Individual.

J. AVAILABILITY OF BOOKS AND RECORDS. etHIN makes its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of the Department of Health and Human Services in the time and manner designated by the Secretary for purposes of determining a Participating Provider's compliance with the Privacy and Security Standards.

K. RETURN OR DESTRUCTION OF PROTECTED HEALTH INFORMATION ON TERMINATION. On termination of a Participation Agreement with a Participating Provider, etHIN returns or destroys all Protected Health Information that etHIN maintains in any form, including any Protected Health Information that is in the possession of Participating Provider's subcontractors or agents (including employees). In such event, etHIN and its subcontractors/agents will retain no copies of such information. If return or destruction is not feasible, etHIN extends the protections of the applicable business associate agreement to such Protected Health Information and limits further use and disclosure of such Protected Health Information to those purposes that make the return or destruction of the information infeasible.

L. SECURITY OBLIGATIONS FOR PROTECTED HEALTH INFORMATION. etHIN, in accordance with the Security Standards and other applicable law, implements administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Health Information it creates, receives, maintains, or transmits on behalf of Participating Providers. etHIN also ensures that any third party, including an agent or subcontractor, to whom etHIN provides Protected Health Information agrees to implement such safeguards by written agreement. If etHIN becomes aware of any Security Incident or any breach of "unsecured Protected Health Information" within the meaning of Section 13402 of HITECH (and any regulations or agency guidance issued pursuant thereto), etHIN promptly reports the same in writing to the applicable Participating Provider.

M. COMPLIANCE WITH FEDERAL SUBSTANCE ABUSE CONFIDENTIALITY REQUIREMENTS. If etHIN is deemed to be a qualified service organization within the meaning of 42 C.F.R Part 2 and receives, stores, processes, or otherwise deals with any patient record maintained in connection with a federally assisted alcohol and drug abuse program, etHIN will comply with 42 C.F.R. Part 2 and, if necessary, resist in judicial proceedings any efforts to obtain access to patient records except as permitted by those regulations.

N. PRIVACY OFFICER. Although etHIN is not a covered entity, etHIN assigns duties traditionally held by a Privacy Officer to one or more of its employees in order to provide oversight for all aspects relating to the privacy of PHI. etHIN's Privacy Officer is responsible for addressing and resolving privacy-related complaints, including ensuring appropriate corrective action occurs; maintaining a log accounting for disclosures of Protected Health Information as necessary to comply with Paragraph H; ensuring appropriate workforce training; and maintaining appropriate documentation of the same. etHIN's Privacy Officer is Kim Dunn, kdunn@ethin.org.

II. HIPAA SECURITY POLICIES

To ensure the confidentiality, integrity, and availability of Electronic Protected Health Information ("EPHI") collected, maintained, used, or transmitted by etHIN, etHIN and/or its contractor(s), as applicable, implement reasonable and appropriate administrative, physical, and technical safeguards meeting the requirements of the Security Standards. etHIN primarily assists with the transfer or EPHI and does not typically maintain, host, or save EPHI, but one or more etHIN contractor(s) may perform such functions. As a result, certain implementation specifications in the Security Standards do not apply directly to etHIN and etHIN relies on its contractor(s) (e.g., SH Data Technologies) to ensure compliance with the applicable specification as appropriate.

A. ADMINISTRATIVE SAFEGUARDS

1. SECURITY MANAGEMENT PROCESS. etHIN implements policies and procedures to prevent, detect, contain, and correct security violations. Specific measures include:

(a) Risk analysis (Required). etHIN periodically conducts accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Electronic Protected Health Information held by etHIN to identify potential security risks and determining the probability of occurrence and magnitude of risks. Although etHIN does not typically hold EPHI, etHIN considers how any Electronic Protected Health Information flows throughout etHIN (including how any EPHI is created, received, maintained, or transmitted; the less obvious sources of EPHI (e.g., telephones, flash drives); appropriate contracting with vendors and consultants that create, receive, maintain or transmit EPHI; and the human, natural, and environmental threats to information systems that contain EPHI).

(b) Risk management (Required). Through implementation of these policies and procedures; the etHIN Data Sharing Agreement and associated Participant Policies and Procedures; appropriate contracting with third parties that maintain or host EPHI (e.g., SH Data Technologies); periodic risk analysis; and workforce training, etHIN implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to (1) ensure the confidentiality, integrity, and availability of electronic protected health information etHIN creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA's Privacy Standards; and (4) ensure compliance with HIPAA's Security Standards by its workforce.

(c) Sanctions policy (Required). etHIN applies appropriate sanctions against workforce members who fail to comply with etHIN's applicable privacy and security policies and procedures. The Privacy Officer, in consultation with etHIN's Executive Director/CEO, establishes a range of sanctions to be imposed if etHIN's HIPAA policies and procedures or the HIPAA privacy and security rules are violated. Disciplinary action is commensurate with the severity of the breach and the degree of potential harm. Sanctions may range from warnings and further training (e.g., in the event an employee was not aware of policy requirements and the effects of the violation are minimal), to immediate termination, either from employment or access to etHIN's health information exchange (e.g., in the event of a knowing and intentional violation). All etHIN workforce members are made aware of the disciplinary actions and sanctions that may be imposed.

(d) Information system activity review (Required). etHIN and/or its contractor(s) implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports. etHIN implements procedures defining access to audit logs, including procedures for patients to access audit log information as required by law. etHIN also proactively reviews available logs and reports from etHIN's contractor, SH Data Technologies. Reports will be shared with Participants on a regular basis, with Security Incidents being reported in an expedited manner.

2. **ASSIGNED SECURITY RESPONSIBILITY.** etHIN has a clearly identified security official ("IT Security Officer") who is responsible for the development and implementation of etHIN's Security Standards policies and procedures. etHIN's IT Security Officer is Pam Matthews, pmatthews@ethin.org. etHIN may, in its discretion, appoint the etHIN Privacy Officer to be the IT Security Officer or may assign these roles to separate individuals. etHIN's IT Security Officer monitors information systems activity and Security Incidents, ensures that appropriate follow-up action occurs (including necessary mitigation and corrective measures), and ensures appropriate implementation of etHIN's HIPAA Security Policies.

3. **WORKFORCE SECURITY.** etHIN implements policies and procedures to ensure that workforce members have appropriate access to Electronic Protected Health Information and to prevent those workforce members who should not have access from obtaining access to Electronic Protected Health Information. Specific measures include:

(a) Authorization and/or supervision (Addressable). etHIN implements procedures for the authorization and/or supervision of workforce members who work with Electronic Protected Health Information or in locations where it might be accessed by requiring its workforce members to sign a confidentiality agreement, comply with applicable law as a condition of employment, and access Protected Health Information only on a need-to-know basis necessary for job function. On commencement of employment, or initiation of a new job function by a workforce member, the etHIN supervisor determines the access to EPHI and systems containing EPHI that is appropriate for the supervised workforce member (e.g., global access; limited access; no access), then coordinates the granting or limiting of such access with etHIN's IT Security Officer to ensure the workforce member's appropriate access.

(b) Workforce clearance procedures (Addressable). etHIN implements procedures to determine that the access of a workforce member to Electronic Protected Health Information is appropriate by assigning the minimum access necessary based on appropriate job descriptions or titles. If an employee's job does not require access to EPHI, no access is granted to that employee. etHIN supervisors are responsible for working with etHIN's IT Security Officer to assign appropriate access levels to supervised employees and to administer access levels, including at the time of job initiation, modification, transfer, and termination.

(c) Modification/Termination procedures (Addressable). etHIN supervisors are responsible for ensuring that supervised workforce members have appropriate access to EPHI and systems containing EPHI. Further, etHIN supervisors are responsible for timely informing the IT Security Officer when an employee's access rights should be modified or terminated. Based on information provided by etHIN supervisors, etHIN's IT Security Officer reviews and updates access levels periodically and as appropriate (e.g., when informed by a supervisor that an employee's job function has changed). Further, etHIN's IT Security Officer terminates access to Electronic Protected Health Information as of the date employment of a workforce member ends or the workforce member no longer requires such access for job functions.

4. INFORMATION ACCESS MANAGEMENT. etHIN implements policies and procedures for authorizing access to Electronic Protected Health Information by its employees and subcontractors that are consistent with the applicable requirements of the Privacy Standards. Specific measures include:

(a) Access authorization (Addressable). etHIN implements policies and procedures for granting access to Electronic Protected Health Information, for example, through access to a workstation, transaction, program, process, or other mechanism.

1. etHIN defines roles available to access the etHIN Network, and the Participating Provider defines jointly with etHIN the roles each Participating Provider's users are assigned to.

2. Access may be based on an individual's licensure status, job-type role within etHIN or a Participating Provider (clinician, support staff, trainer, etc.), purposes of the access or query, or other categories.

3. etHIN applies the standard of "minimum access required" in regard to access to Electronic Protected Health Information or other categories of data or queries of the etHIN network, such as the rights for use of the system for technical support, administrative access for audit and legal compliance purposes, emergency access or access to sensitive data. No user is assigned a role with higher rights or access than is required for his or her role within a Participating Provider or etHIN.

(b) Access establishment and modification (Addressable). etHIN implements policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

1. etHIN grants access to Participating Providers requesting such access to Electronic Protected Health Information only for the permitted purposes described in etHIN's Participating Provider Policies.

2. Requests to grant access to potential users of the etHIN HIE network must be in writing utilizing the appropriate etHIN eHIP User Setup Form. Granting of access and security clearances without appropriate documentation is prohibited.

3. Participating Providers' usage activity will be monitored, and Participating Providers' users will be notified according to the following guidelines: Communicate to Participating Providers when activated credentials have been inactive for a period of 60 days, at which time the account will be suspended, and notified again at 120 days if still inactive, at which time the account will be terminated. A suspended account is an activated account whose credentials have been unused for 60 days. A terminated account is an activated account whose credentials have been unused for 120 days. An inactive account is an account whose credentials have been issued to a user, but the user has not initially used, or activated, the credentials within 30 days, at which time the account is suspended. etHIN performs this review and notification process not less than weekly.

5. SECURITY AWARENESS AND TRAINING. etHIN implements a security awareness and training program for all members of its workforce (including management). Specific measures include:

(a) Security reminders (Addressable). etHIN's IT Security Officer periodically distributes bulletins regarding identified security issues and reminders regarding the requirements of the HIPAA Privacy and Security Standards to workforce members and etHIN Participants. etHIN's IT Security Officer maintains documentation of such reminders consistent with the requirements of this policy.

(b) Protection from malicious software (Addressable). etHIN and its contractor, SH Data Technologies, establish procedures for guarding against, detecting, and reporting malicious software by utilizing software that identifies and reports such software. For example, SH Data Technologies installs the current versions of Anti-Malware Software on all production, development, and test servers and on all user workstations. etHIN's IT Security officer and etHIN's contractor, SH Data Technologies, routinely monitor and address malware alerts, scan for, address, and remove threats, and apply appropriate security patches, as necessary. Because malicious software is frequently brought into an organization through email attachments and programs downloaded from the Internet, etHIN trains its workforce regarding its role in protecting against malicious software and system protection capabilities.

(c) Log-in monitoring (Addressable). etHIN's contractor, SH Data Technologies, records and monitors etHIN log-in attempts and locks out users after a set number of log-in attempts.

(d) Password management (Addressable). etHIN workforce members are prohibited from sharing passwords with each other. Further, etHIN requires that (1) each password to be composed of a minimum of eight (8) alphanumeric characters and modified every one hundred eighty (180) days; and (2) workforce members and Participating Providers keep passwords confidential and secure.

6. SECURITY INCIDENT POLICIES AND PROCEDURES. etHIN and its contractor(s) implement policies and procedures to address Security Incidents. Specific measures could include but are not limited to identifying, logging, and responding to suspected or known Security Incidents; mitigating, to the extent practicable, harmful effects of Security Incidents that are known to the etHIN; and documenting Security Incidents and their outcomes. All known or suspected Security Incidents shall be reported to etHIN's IT Security Officer. etHIN's IT Security Officer shall respond to all suspected Security Incidents, including preserving evidence; mitigating, to the extent possible, the situation that caused the incident; documenting the incident and the outcome; and evaluating security incidents as part of ongoing risk management. etHIN's IT Security Officer is responsible for establishing adequate response and reporting procedures for Security Incidents, including breach reporting required by §§ 45 C.F.R. 164.402 through 414 and Tennessee Code Annotated § 47-18-2107 (such notifications generally must be provided without unreasonable delay and within certain time periods).

7. CONTINGENCY PLAN. etHIN establishes (and implements as needed) contracts, policies, and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain Electronic Protected Health Information either directly or with appropriate business associates. etHIN does not typically host or store EPHI and arranges for reasonable backup and archival policies described as follows:

(a) Data backup plan (Required). etHIN arranges for etHIN's contractor, SH Data Technologies, to establish and implement procedures to create and maintain accessible exact copies of stored or hosted Electronic Protected Health Information.

(b) Disaster recovery plan (Required). etHIN arranges for etHIN's contractor, SH Data Technologies, to establish and implement procedures to restore loss of stored or hosted data. Timeframes for recovery are governed by the SH Data Technologies Agreement.

(c) Emergency mode operation plan (Required). etHIN arranges for etHIN's contractor, SH Data Technologies, to establish and implement procedures to enable continuation of critical business processes for protection of the security of Electronic Protected Health Information while operating in emergency mode.

(d) Testing and revision procedures (Addressable). etHIN arranges for etHIN's contractor, SH Data Technologies, to implement procedures for periodic testing and revision of contingency plans.

(e) Applications and data criticality analysis (Addressable). etHIN arranges for etHIN's contractor, SH Data Technologies, to assess the relative criticality of specific applications and data in support of other contingency plan components.

8. EVALUATION. etHIN performs a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Standards and subsequently, in response to environmental or operational changes affecting the security of Electronic Protected Health Information, that establishes the extent to which etHIN's security policies and procedures meet the requirements of the Security Standards. To this end, etHIN shall review this policy at least once every three years and implement appropriate updates and revisions.

9. BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS. etHIN identifies all business associates, as defined by the Privacy and Security Standards. To the extent required by law, etHIN enters into agreements with third parties that create, receive, maintain, or transmit Electronic Protected Health Information on behalf of etHIN, requiring such third parties to comply with the applicable requirements of the Security Standards, implement reasonable and appropriate safety measures to protect the information, ensure that any agent (e.g., employee or partner) or subcontractor to whom it provides this information agrees to implement reasonable and appropriate safety measures to protect it; and report to etHIN any Security Incident of which it becomes aware, including breaches of unsecured Protected Health Information.

B. PHYSICAL SAFEGUARDS

1. ACCESS CONTROLS. etHIN implements contracts, policies, and procedures to limit physical access to its electronic information systems and the offices or in which they are housed, while ensuring that properly authorized access is allowed. Specific measures include:

(a) Contingency operations (Addressable). Because etHIN does not typically host or store EPHI, etHIN arranges through its contractor, SH Data Technologies, to establish and implement reasonable procedures that allow office or facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(b) Security plan (Addressable). etHIN implements policies and procedures to safeguard its office and the equipment therein from unauthorized physical access, tampering, and theft by ensuring external doors are locked and workstations with access to EPHI are appropriately monitored and not available for access by unauthorized parties. Encryption tools are used on all etHIN workstations.

(c) Access control and validation procedures (Addressable). etHIN implements procedures to control and validate a person's access to etHIN's facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision etHIN's IT Security Officer shall determine in all cases whether third-party access to software programs for testing and revision is appropriate. Such third-party access must be requested in a written request submitted directly to etHIN's IT Security Officer and approved by such Security Officer prior to access.

(d) Maintenance records (Addressable). etHIN's IT Security Officer documents repairs and modifications to the physical components of the etHIN office which are related to security (for example, hardware, walls, doors, and locks) and maintains a log of the same consistent with the document retention requirements of this policy.

2. WORKSTATION USE. etHIN implements policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access Electronic Protected Health Information. etHIN workforce members shall ensure that workstations are not accessible to unauthorized parties by logging off when a workstation is not in use. Workstations will automatically lock after a thirty-minute period of inactivity. Off-site workstations shall be subject to the same controls and restrictions as on-site workstations (e.g., system time-outs; privacy screens; and logoffs).

3. WORKSTATION SECURITY. etHIN identifies all workstations with access to EPHI (including remote access computers) and implements physical safeguards for all workstations that access Electronic Protected Health Information, to restrict access to authorized users. If a laptop is to be used for remote access to Electronic Protected Health Information, multi-factor authentication will be required (e.g., name and password plus "challenge" questions). If Electronic Protected Health Information is stored on a laptop, both multi-factor authentication and whole disk encryption are required.

4. DEVICE AND MEDIA CONTROLS. etHIN does not typically host or store EPHI and therefore arranges with its contractor, SH Data Technologies, for implementation of procedures that govern the receipt and removal of hardware and electronic media that contain Electronic Protected Health Information into and out of an office or facility, and the movement of these items within the office or facility. Specific measures include:

(a) Disposal (Required). etHIN arranges through its contractor, SH Data Technologies, for implementation of procedures to address the final disposition of Electronic Protected Health Information, and/or the hardware or electronic media on which it is hosted or stored. All discarded electronic media containing EPHI shall be destroyed to ensure the EPHI is unusable and/or inaccessible (e.g., by degaussing; burning, etc.).

(b) Media re-use (Required). etHIN arranges through its contractor, SH Data Technologies, for permanent removal of Electronic Protected Health Information from electronic media before the media are made available for re-use.

(c) Accountability (Addressable). etHIN arranges through its contractor, SH Data Technologies, for maintenance of a record of the movements of hardware and electronic media and any person responsible therefor. By policy, etHIN's contractor, SH Data Technologies, logs hardware movement into and out of SH Data Technologies facilities and sanitizes data and hard drives before disposal or re-use.

(d) Data backup and storage (Addressable). etHIN arranges through its contractor, SH Data Technologies, for creation of a retrievable, exact copy of Electronic Protected Health Information, when needed, before movement of equipment.

C. TECHNICAL SAFEGUARDS

1. ACCESS CONTROL. etHIN enters into contracts and implements technical policies and procedures for electronic information systems that maintain Electronic Protected Health Information to allow access only to those persons or software programs that have been granted access rights as specified in etHIN policies. Specific measures include:

(a) Unique user identification (Required). etHIN assigns a unique name and/or number for identifying and tracking user identity.

(b) Emergency access procedure (Required). etHIN and/or its contractor(s) establish (and implements, as needed) procedures for obtaining necessary Electronic Protected Health Information during an emergency.

(c) Automatic logoff (Addressable). etHIN arranges through a contractor for implementation of electronic procedures that terminate an electronic session after a predetermined time of inactivity. This is a global configuration item for all users.

(d) Encryption and decryption (Addressable). etHIN's contractor, SH Data Technologies, which holds all EPHI to which etHIN has access, implements mechanisms to encrypt and decrypt Electronic Protected Health Information that is live, at rest, and backed up.

(e) Training). etHIN implements training to ensure that all individuals with permission to view Electronic Protected Health Information within etHIN undergo a minimum level of training. The initial training includes etHIN system training, compliance training related to etHIN's policies, and the user's responsibilities under the Authorized User/Designee Agreement and etHIN's Participating Policies and Procedures. After initial user onboarding and training, etHIN will provide additional training to participant end users regarding the etHIN system as needed. etHIN compliance training is required annually for all users. Participating Providers are responsible for training their employees on federal and state privacy regulations (HIPAA).

2. AUDIT CONTROLS. etHIN implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use Electronic Protected Health Information. Specific measures include:

(a) Intersystems HealthShare Usage Reports. Through the Intersystems HealthShare Usage Reports, etHIN monitors access to all Electronic Protected Health Information. Audit logs of accessed data can be made available through printed reports. These audit logs will contain data on how information is accessed. The following information is captured and available:

(1) Information accessed on a patient (information accessed for a specific patient)

(2) Information accessed by provider (information accessed by a specific provider)

(3) IHE Audit Information (information accessed by individual IHE Audit trial and node authentication (ATNA) transactions)

(b) etHIN determines a minimum system activity audit functions and monitoring elements consistent with federal and state guidelines. Audit trails of these elements and activities are preserved in a manner that prevents changing or tampering with the content. All access to the audit logs is also audited.

(c) etHIN monitors and conducts reviews of audit logs daily for user lockouts and other significant events. Further, etHIN implements a monitoring process to identify unusual activities and take appropriate action.

(d) etHIN has a process in place that facilitates audits of transactions between itself and other exchanges/RHIOs.

(e) Access to audits are based on a written request through a process as determined by etHIN. etHIN provides audit logs as required by law and permits the following persons access to audit logs: etHIN staff members assigned to audit logs, IT Security Officer, Privacy Officer.

(f) etHIN retains audit logs consistent with the requirements of state and federal laws, rules, regulations, and contracts.

3. INTEGRITY. etHIN arranges through its contractor, SH Data Technologies, to protect Electronic Protected Health Information from improper alteration or destruction. Specific measures include:

(a) Mechanism to Authenticate Electronic Protected Health Information (Addressable). etHIN's contractors(s) implement electronic mechanisms to corroborate that Electronic Protected Health Information has not been altered or destroyed in an unauthorized manner.

4. PERSON OR ENTITY AUTHENTICATION. etHIN implements procedures to verify that a person or entity seeking access to Electronic Protected Health Information is the one claimed by ensuring unique user identification through contracts with Participating Providers.

(a) Strong authentication measures. etHIN uses best practice measures to verify the identity of a person or entity seeking access to Electronic Protected Health Information, which, at a minimum may include single or multi-factor authentication, additional security questions, use of trusted networks, authentication attempts management ("3 strikes = lockout"), session timeouts, and password management system.

(b) Secure connectivity required. etHIN implements security measures to ensure that connections between a Participating Provider and etHIN's Network makes use of a secure technical method, such as Virtual Private Network (VPN) tunnels, to connect and share data across un-trusted network links (such as the Internet). Acceptable methods for data exchange must provide for authentication of each end point of the connection and securely encapsulate the data traffic/transmission. etHIN provides each Participating Provider with specific VPN implementation and configuration information. Documentation regarding connections to the etHIN Network are treated as restricted information and managed with appropriate security measures to ensure that only authorized employees of the Participating Providers have access to this information.

(c) Password management. The etHIN Domain Administrators and etHIN-HIE Domain Administrators are responsible for the creation and deletion of user accounts on the network. All approved etHIN users will be provided individual security credentials for access. The use of group or profile logins will not be permitted. User accounts will be configured with passwords. Password policy rules will include as a minimum:

- Unique user IDs and passwords will be required
- Passwords will be a minimum length of at least eight (8) alpha-numeric characters
- Complexity will be required
- Maximum password age will force users to change every 365 days
- New accounts will require the user to immediately change the temporary password provided at setup
- Users will be locked out after three incorrect login attempts.
- Network settings will require the administrator to reset locked out users
- The password history will be set to remember at least 12 passwords
- Any user or profile not meeting these standards will be approved in writing by the etHIN HIE Administrator
- 'Store password using reversible encryption' will be disabled
- Authentication attempts and Login events will be tracked
- Failed authentication attempts resulting in lockouts will be audited

(d) Failed authentications. etHIN implements electronic procedures that lockout a user after a specified number of failed authentication attempts. etHIN implements procedures that log and track all failed authentication attempts and lockouts.

5. TRANSMISSION SECURITY. Through its contractor(s), etHIN implements technical security measures to guard against unauthorized access to Electronic Protected Health Information that is being transmitted over an electronic communications network. Specific measures include:

(a) Integrity controls (Addressable). Security measures to ensure that electronically transmitted Electronic Protected Health Information is not improperly modified without detection until disposed of.

(b) Encryption (Addressable). etHIN's contractor, SH Data Technologies, which holds all Electronic Protected Health Information to which etHIN has access, encrypts Electronic Protected Health Information at rest, in motion, and in back-up. Any e-mail communications initiated by etHIN that contain Electronic Protected Health Information are sent through an encrypted e-mail service (e.g., DataMotion Secure, or similar).

D. POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

1. POLICIES AND PROCEDURES. etHIN implements reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Standards. etHIN may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the Security Standard.

2. DOCUMENTATION. etHIN maintains the policies and procedures implemented to comply with the Security Standards in written (which may be electronic) form; and, if an action, activity or assessment is required by the Security Standards to be documented, etHIN maintains a written (which may be electronic) record of the action, activity, or assessment. Specific measures include:

(a) Time limit (Required). etHIN retains such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

(b) Availability (Required). etHIN makes documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(c) Updates (Required). etHIN reviews documentation periodically, and updates as needed, in response to environmental or operational changes affecting the security of the Electronic Protected Health Information.

III. DEFINITIONS.

Terms (including capitalized terms) used, but not otherwise defined in this Policy have the meaning assigned by the Privacy and Security Standards, as amended and updated from time to time. Each of the following terms is construed in accordance with the following:

"Individual" has the same meaning as "individual" in 45 C.F.R. § 160.103 and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

"Participating Provider" means all organizations and practitioners connected to etHIN for the purposes of health information exchange through etHIN.

"Privacy Standards" means the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. parts 160 and 164, as amended from time to time.

"Protected Health Information" has the same meaning as "protected health information" in 45 C.F.R. § 160.103, limited to Protected Health information from, or created or received by etHIN on behalf of, the applicable Participating Provider. Protected Health Information includes Electronic Protected Health Information, as defined by the 45 C.F.R. § 160.103.

"Required by Law" has the same meaning as that contained in 45 C.F.R. § 164.103 and shall include, but not be limited to, the provisions of the 21st Century Cures Act and regulations issued pursuant thereto applicable to "health information exchanges" as defined therein.

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. The following are examples of Security Incidents: stolen or otherwise inappropriately obtained passwords that are used to access EPHI; corrupted backup tapes that do not allow restoration of EPHI; virus attacks that interfere with the operations of information systems with EPHI; physical break-ins leading to the theft of media with EPHI; failure to terminate the account of a former employee that is then used by an unauthorized user to access information systems with EPHI; providing media with EPHI, such as a PC hard drive or laptop, to another user who is not authorized to access the EPHI prior to removing the EPHI stored on the media.

"Security Standards" means the Standards for Security of Electronic Protected Health Information, 45 C.F.R. parts 160 and 164, as amended from time to time.

IV. DOCUMENTATION.

This version of the policy, together with any forms and other documentation obtained in accordance with the policy, shall be retained for a minimum of six years from the date of last use.