TEXAS HEALTH SERVICES AUTHORITY
MODEL POLICIES
REGARDING THE SECURITY OF HEALTH INFORMATION

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

TABLE OF CONTENTS

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law..

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law..

ARTICLE I – INTRODUCTION

The Texas Health Services Authority (THSA) Health Information Model Policy Regarding Privacy and Security of Health Information is hereby adopted and approved by THSA, and it shall be effective as of the Effective Date. The Model Policy is comprised of two separate sets of policies: a set of Model Privacy Policies and a set of Model Security Policies. This document contains the Model Security Policies; the Model Privacy Policies are contained in an accompanying document.

Capitalized terms used herein are defined in Article II, Definitions.

The THSA: Background. By enacting Chapter 182 of the Texas Health and Safety Code, the Legislature of the State of Texas established THSA as a "public-private collaborative" to develop "a seamless electronic health information infrastructure to support the health care system in the state and to improve patient safety and quality of care."[1] Pursuant to this directive, THSA plans to offer statewide health information exchange capacity through a network called HIETexas for the purposes of: (i) enabling the sharing of patient information between providers across the state via HIEs and their Participants; and (ii) eventually linking with other statewide HIEs on a national level via participation in the eHealth Exchange (formerly known as the Nationwide Health Information Network or NwHIN).

In 2010, the Department of Health and Human Services, through the Office of the National Coordinator for Health Information Technology, approved Texas' Strategic and Operational Plan for Statewide HIE, under which the state received grant funding to further certain health information exchange goals. As part of this program, which is being administered by the Texas Health and Human Services Commission (HHSC) with contractual support from the THSA, the HHSC helped to fund 12 regional HIE networks, the Local HIEs, which cover approximately 90% of the state's physicians and hospitals eligible for the program. The purpose of the Model Policy is to help the Local HIEs comply with state and federal law requirements by providing a guide as to some common policies and procedures that may be applicable to the HIEs.

HIE Models. An HIE may take one of several architectural approaches, which will dictate to some extent the number and types of privacy and security policies needed by the HIE. In general, Local HIEs will take one of the following two approaches, or some combination of these approaches:

> Federated. A Local HIE that provides organizational control of the health information and provides the framework for data-sharing capability to organizations widely distributed across a local or regional HIE. This model allows the data source organizations to manage and store the patient health information and indices. When requested, data is queried from the data source organization and not stored centrally. Local HIEs that meet this definition are referred to in the Model Policy as "Federated HIEs."

[1] *See* TEX. HEALTH AND SAFETY CODE § 182.001.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Centralized. A Local HIE that requires organizations to send patient demographic and clinical health information to a shared repository. This centralized repository is queried to obtain a patient's health information and other indices, and usually acts as the authoritative source of the requested data.

Hybrid. A Hybrid HIE incorporates aspects of both a federated and a centralized architecture model.

Business Associates. The HITECH Act extended the security requirements of HIPAA to Business Associates of Covered Entities. In the HIPAA Omnibus Rule, the Office for Civil Rights specified that a health information organization, or HIE, is a Business Associate under HIPAA.[2] Therefore, HIEs must comply with the elements of the Privacy and Security Rules that apply to Business Associates under HIPAA and HITECH.

A Business Associate's access, use, and disclosure of EPHI obtained from or created pursuant to the relationship with a particular Participant is governed and limited primarily by the Business Associate Agreement and any other participation or services agreement executed with that Participant. Most HIEs will have both a Business Associate Agreement and what is generally called a "Participation Agreement," or sometimes a service agreement, with its Participants. The Participation Agreement is the agreement between the HIE and its Participants that, along with the Business Associate Agreement, spells out the rights and responsibilities of each party with respect to the business relationship as well as the privacy and security responsibilities of the parties with respect to EPHI.

A model Business Associate Agreement is attached as Appendix A-1 to the Model Privacy Policies (Sample Participant Business Associate Agreement). This model Business Associate Agreement was approved by the THSA board following a stakeholder comment and review process, and was disseminated to the Local HIEs in March 2012; updates were made to the model Business Associate Agreement in March 2013 to reflect changes made in the HIPAA Omnibus Rule. As HIEs may also require the assistance of one or more Subcontractors, such as software vendors, HIEs should also require such Subcontractors to execute Business Associate Agreement, which is intended to further ensure the privacy and security of EPHI. Note that the sample agreement should be modified as appropriate to reflect the actual use, situation and relationship between the HIE and its Participants and Subcontractors. Local HIEs should consult their legal counsel to ensure appropriate use of the model agreements.

THSA Model Security Policies. These Model Security Policies are not intended to be exhaustive or one-size-fits-all, and Local HIEs are not required to adopt them verbatim; rather, the Model Security Policies are intended to serve as a model set of policies that Local HIEs can adopt or use as a resource to ensure the privacy and security of EPHI.

[2] *See* 45 C.F.R. §§ 160.103.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

THSA realizes that some Local HIEs may have robust policies already in place, while other Local HIEs may not, and that the degree and manner of access, disclosure, and use of EPHI by Local HIEs throughout the state varies considerably. Thus, while these Model Security Policies often contain detailed, specific procedures and protocols, each Local HIE has the freedom and flexibility to implement its own unique privacy and security measures as appropriate and in compliance with state and federal law.

Both state and federal laws implicate the security and privacy of EPHI, and the Model Policy was developed to comply with applicable law and to implement best practices. Thus, Local HIEs may choose to adopt these Model Security Policies in their entirety, or to use them as a resource to facilitate development of their own privacy measures. However, the law in this area continues to evolve, and thus it will be important for Local HIEs to continually stay abreast of applicable law and industry standards.

In deciding which security measures to use, HIE must take into account the following factors:

1. the size, complexity, and capabilities of the HIE;

2. HIE's technical infrastructure, hardware, and software security capabilities;

3. the costs of Security measures; and

4. the probability and criticality of potential risks to electronic protected health information.

Security Safeguards. The security implementation specifications set forth in the HIPAA Security Rule can broadly be broken down into three categories: Administrative Safeguards, Physical Safeguards and Technical Safeguards. Under the HIPAA Omnibus Rule, which took effect on March 26, 2013, Business Associates, such as HIEs, must comply with these safeguards beginning September 23, 2013.

Administrative Safeguards. Administrative safeguards are administrative actions, policies, and procedures that manage the selection, development, implementation, and maintenance of security measures to protect EPHI and to manage the conduct of Users, some of which apply to HIE Users and/or Participant Users, in relation to the protection of such EPHI.[3] These Model Security Policies are considered to implement the administrative safeguards below:

- Security Management Process;
- Assigned Security Responsibility;
- Workforce Security;

[3] *See* 45 C.F.R. §§ 164.304 and 164.308.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

- Information Access Management;
- Security Awareness and Training;
- Security Incident Procedures;
- Contingency Plan;
- Evaluation; and
- Business Associate Contracts and Other Arrangements.

Technical Safeguards. A Technical Safeguard is the technology and the policy and procedures for its use that protect EPHI and control access to it.[4] These Model Security Policies are considered to implement the Technical Safeguards below, certain of which may be applicable to HIE Users, Participant Users, or both:

- Facility Access Controls;
- Workstation Use;
- Workstation Security; and
- Device and Media Controls.

Physical Safeguards. Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.[5] These Model Security Policies are considered to implement the following physical safeguards:

- Access Control;
- Audit Controls;
- Integrity;
- Person or Entity Authentication; and
- Transmission Security.

Required vs. Addressable Security Implementation Specifications. Pursuant to federal law, certain of the Administrative Safeguards, Technical Safeguards, and Physical

[4] *See* 45 C.F.R. §§ 164.304 and 164.312
[5] *See* 45 C.F.R. §§ 164.304 and 164.310

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Safeguards are Required while others are Addressable.[6] Each policy in these Model Security Policies contains a text box clearly designating the specification as Required or Addressable.

Required. If a security implementation specification is required, HIE must implement the specification as the HIPAA Security Law provides.

Addressable. If a security implementation specification is addressable, HIE may consider the implementation specification against other alternatives based upon the size, complexity, and capability of HIE. **Note, however, that Addressable security implementation specifications are not optional.**

FAILURE OF AN HIE TO IMPLEMENT AN ADDRESSABLE IMPLEMENTATION SPECIFICATION WHERE IT IS REASONABLE OR APPROPRIATE, TO IMPLEMENT A REASONABLE AND APPROPRIATE EQUIVALENT MEASURE, AND/OR FAILURE TO DOCUMENT ITS REASONS FOR NOT IMPLEMENTING AN ADDRESSABLE IMPLEMENTATION SPECIFICATION, AS DESCRIBED BELOW, MAY SUBJECT THE HIE TO SANCTIONS, PENALTIES, AND FINES.

With respect to an Addressable specification, HIE MUST:

(i) Assess whether the implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting HIE's EPHI;

(ii) Implement the specification if reasonable and appropriate; or

(iii) If not reasonable and appropriate:

(a) Document the rational supporting the decision; and

(b) Implement an equivalent alternative measure that is reasonable and appropriate and would accomplish the same purpose; or

(c) Not implement the Addressable implementation specification or an equivalent alternative measure, if the standard could still be met, and implementing the specification or an alternative would not be reasonable or appropriate.

If a given Addressable implementation specification is determined to be reasonable and appropriate, HIE MUST consider options for implementing it. The decision regarding which security measures to implement to address the standards and implementation specifications will depend on a variety of factors, including:

(i) HIE's risk analysis of any current circumstances that leave HIE open to unauthorized access and disclosure of EPHI;

[6] *See* 45 C.F.R. § 164.306(d).

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

(ii) HIEs security analysis of what security measures are already in place or could reasonably be put in place; and

(iii) HIE's financial analysis of how much implementation will cost.

Please Note: Certain policies in these Model Security Policies contain terms in bold and brackets (e.g. **[5]** days or **[human resources department]**). The bold and brackets are meant to denote that such terms are recommended or suggested, but not required.

Federal vs. Texas Authority. Although state law specifically addresses the privacy of EPHI via the Texas Medical Records Privacy Act and other statutes and codes that regulate certain sources and types of EPHI that are subject to additional privacy protection, Texas law does not have a statutory equivalent to the HIPAA Security Rule. Thus, these Model Security Policies are intended to track the requirements of HIPAA and the HITECH Act and implementing regulations. However, please note that in the event that state law provides for greater protections or privacy rights with respect to EPHI, pursuant to analysis under 45 C.F.R. Chapter 160, Subpart B, state law shall preempt HIPAA.

On October 12, 2012, pursuant to Chapter 182 of the Texas Health and Safety Code as amended during the 82nd Legislative Session, HHSC proposed new provisions to the Texas Administrative Code (1 TEX. ADMIN. CODE §§ 390.1 and 390.2) concerning standards related to the electronic exchange of health information. The new rules may alter definitions in this Model Policy, and thus it would be prudent for Local HIEs to monitor the status of this legislation.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE II – DEFINITIONS

Unless otherwise provided, the following definitions in this Article II shall be used in the interpretation of these Model Security Policies:

Access – means the ability or the means necessary to read, write, modify, or communicate data or information or otherwise use any system resource.

Addressable – means an implementation specification that: (i) should be assessed to determine if it is a reasonable and appropriate safeguard in its environment, when analyzed with reference to its likely contribution to protecting HIE's EPHI; (ii) should be implemented if reasonable or appropriate; or (iii) if not reasonable and appropriate, may be substituted for an equivalent alternative measure if such alternative is reasonable or appropriate. HIE must document why it would not be reasonable and appropriate to implement the Addressable specification; see "Required vs. Addressable Security Implementation Specifications" in Article I, Introduction for the further detail on the documentation requirements.

Administrative Safeguards – means administrative actions and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect EPHI and to manage the conduct of HIE's workforce in relation to the protection of EPHI.

Authentication – means corroboration that a person is the one claimed.

Availability – means the property that data or information is accessible and useable upon demand by an authorized person.

Business Associate – means a person or organization who on behalf of a Covered Entity creates, receives, maintains, or transmits protected health information for a function or activity regulated by HIPAA or, as a non-employee of the Covered Entity, provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to a Covered Entity where disclosure of protected health information is required to complete the aforementioned activity. When a Covered Entity discloses EPHI to a Business Associate, a Business Associate Agreement between the Covered Entity and the person or organization performing functions on behalf of the Covered Entity or specified services is required to protect the use and disclosure of EPHI. In the HIPAA Omnibus Rule, the OCR specified that an HIE is a Business Associate.

Business Associate Agreement – means the agreement which contains the requirements set forth in 45 C.F.R. § 164.504(e) entered into between a Covered Entity and a Business Associate or between a Business Associate and a Subcontractor that will be transmitting, accessing, or handling PHI/EPHI on behalf of the Covered Entity.

Centralized HIE - A Local HIE that requires organizations to send patient demographic and clinical health information to a shared repository. This centralized repository is queried to obtain a patient's health information and other indices, and usually acts as the authoritative source of

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

the requested data.

Confidentiality – means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity – means a health plan, health care clearinghouse, and a healthcare provider who transmits any health information in electronic form in connection with a transaction covered under the Privacy Standards or Security Standards. **NOTE: The term "Covered Entity," unless otherwise specified in these policies, shall mean a HIPAA "Covered Entity," as defined at 45 C.F.R. § 160.103. This term is narrower than the definition of "Texas Covered Entity" (defined below).**

Electronic Media – means: (i) electronic storage media on which data is or may be recorded electronically including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (ii) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet, or intranet leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Encryption – means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

EPHI – means electronic protected health information; that is, protected health information that is transmitted by electronic media or maintained in electronic media.

Facility – means the physical premises and the interior and exterior of a building(s).

Federated HIE - A Local HIE that provides organizational control of the health information and provides the framework for data-sharing capability to organizations widely distributed across a local or regional HIE. This model allows the data source organizations to manage and store the patient health information and indices. When requested, data is queried from the data source organization and not stored centrally.

HIE – means a local health information exchange.

HIETexas - the health information exchange for the State of Texas, which is established and operated by THSA.

HIE User(s) – means any employee, vendor, contractor, consultant, etc. who has been authorized to and does access EPHI.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

HIPAA – means the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations which include the Standards for the Privacy of Individually Identifiable Information, codified at 45 C.F.R. Parts 160 and 164) and the Security Standards for the Protection of Electronic Protected Health Information, codified at 45 C.F.R. Parts 160 and 164, as amended by applicable provisions of the Health Information Technology for Economic and Clinical Health Act (Title XIII, Subtitle D) and its implementing regulations.

HIPAA Security Rule – means the Security Standards for the Protection of Electronic Protected Health Information, codified at 45 C.F.R. Parts 160 and 164.

HITECH Act – means the Health Information Technology for Economic and Clinical Health Act (Title XIII, Subtitle D) and its implementing regulations.

Hybrid HIE – Incorporates aspects of both a federated and a centralized architecture model.

Information System – means an interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, information, data, applications, communications, and people. HIE is an Information System.

Integrity – means the property that data or information has not been altered or destroyed in an unauthorized manner.

Local HIE -- means one of the 12 regional HIE networks that cover approximately 90% of the state's physicians and hospitals eligible for the statewide information exchange program.

Malicious Software – means software, such as a virus, which is designed to damage or disrupt a system.

Model Policy – means the Texas Health Services Authority Health Information Model Policy Regarding Privacy and Security of Health Information.

Model Privacy Policies – means the sample privacy policies of the THSA.

Model Security Policies – means the sample security policies contained herein.

Participant – means an individual or entity that accesses, receives, or transmits EPHI to and from the Local HIE.

Participation Agreement - Agreement between an HIE and its Participants which details the rights and responsibilities of each party.

Participant User(s) – means an employee or other person authorized by Participant to access or transmit information to or receive information from the HIE's system.

Password – means Confidential authentication information composed of a string of characters.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

PHI – means protected health information, as defined in 45 CFR § 160.103.

Physical Safeguards – means physical measures, policies, and procedures to protect HIE's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Privacy Standards -- means the standards for the Privacy of Individually Identifiable Information set forth in 45 C.F.R. Parts 160 and 164.

Required – means an implementation specification that must be implemented as set forth in the HIPAA Security Rule.

Security or Security Measures – means all of the Administrative Safeguards, Physical Safeguards, and Technical Safeguards in an Information System.

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.

Security Officer – means an information official who accepts the responsibility of managing and supervising data protection via the use of security measures and the conduct of personnel.

Security Standards -- means the standards for the Security of Individually Identifiable Information set forth in 45 C.F.R. Parts 160 and 164.

Subcontractor – means a person or entity to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Technical Safeguards – means the technology and the policies and procedures for its use that protect EPHI and control access to it.

Texas Covered Entity – means a person as defined by TEX. HEALTH & SAFETY CODE § 181.001(b)(2).

THSA – means The Texas Health Services Authority created by Chapter 182 of the Texas Health and Safety Code.

User(s) – means a person or entity with authorized access; collectively, HIE Users and Participant Users are Users.

Workforce – means employees and other persons whose conduct, in the performance of work for a Covered Entity or HIE, as applicable, is under the direct control of such entity, whether or not they are paid by the Covered Entity or HIE, as applicable.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Workstation – means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

If any term defined under this Article II is also defined under HIPAA or the privacy laws of the State of Texas, then the definition in HIPAA or the Texas privacy laws shall prevail based on HIPAA preemption principles. If any term in these Model Security Policies is not defined in this Article II but is defined under HIPAA or the privacy laws of the State of Texas, then that term shall have the definition prescribed under HIPAA or the Texas state law based on HIPAA preemption principles. If any term in these Model Security Policies is not defined by either this Article II, HIPAA or the privacy laws of the State of Texas, then it shall be defined by its normal and customary meaning with preference given to the meaning that creates the most privacy and security of EPHI.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE III - POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

IMPLEMENTATION SPECIFICATIONS

This standard is REQUIRED by 45 C.F.R. § 164.316

POLICY

HIE shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements set forth in the applicable provisions of HIPAA and the HITECH Act.

PROCEDURE

1. HIE shall maintain such policies and procedures in written (which may be electronic) form.

2. HIE may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with applicable law.

3. If an action, activity or assessment is required to be documented, maintain a written (which may be electronic) record of the action, activity or assessment.

4. HIE shall maintain the documentation of its policies for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

5. HIE shall make the documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

6. HIE shall review documentation periodically and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

CITATIONS

45 C.F.R. § 164.316

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE IV – SECURITY OFFICER

IMPLEMENTATION SPECIFICATIONS

This standard is REQUIRED by 45 C.F.R. § 164.308(a)(2)

POLICY

HIE shall designate a Security Officer whose role shall be developing, implementing, maintaining, and monitoring HIE's adherence to the terms of its security policies.

Editor's Note: Depending on the size and resources of the HIE, the Security Officer may be an individual with multiple titles and/or roles.

PROCEDURE

1. Documentation of such designation shall be regularly updated and maintained.

2. HIE may require Security Officer to perform specific duties in the management and supervision of HIE's security measures in order to maintain the protection of EPHI by Users. Such duties *may* include one or more in the following *non-exhaustive* list or the delegation of such, either in whole or in part:

   (a) Issuing access authorization;

   (b) Modifying or terminating access authorization as positions change;

   (c) Password management;

   (d) Overseeing data backup and access to data during emergencies;

   (e) Preventing, detecting, and mitigating viruses;

   (f) Reviewing technical controls such as the adequacy of firewalls;

   (g) Overseeing the security training of HIE Users;

   (h) Monitoring logs and reports of network access;

   (i) Supervising and sanctioning HIE Users in connection with security issues;

   (j) Overseeing security breach responses;

   (k) Overseeing Security Incident responses; and

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

(l) Evaluating HIE's continued compliance with the security standards.

3. HIE may require Security Officer to report on a periodic basis to HIE's **[Board of Directors, Chief Executive Officer, Administrator, HIPAA task force, or other supervising person or group depending on the size of the HIE]** regarding the Security Officer's responsibilities.

4. HIE's Security Officer may, from time to time, delegate to any other person or organization any of his or her duties and responsibilities per HIE policies. **Upon designation and acceptance of such delegation, employment, or authorization, the Security Officer shall have no liability for the acts or omissions of any such designee so long as the respective Security Officer does not violate any fiduciary responsibility to HIE in making or continuing such designation.** The Security Officer may, from time to time, review all delegations of responsibility, and those delegations shall be terminable upon notice if Security Officer, in his or her sole discretion, deems reasonable and prudent under the circumstances.

5. In order to fulfill its responsibilities, HIE's Security Officer may collaborate with HIE's Privacy Officer, legal counsel, contact person, **[human resources department, information technology or information systems departments]**, and/or any other person whom the Security Officer in his or her sole discretion deems prudent to consult.

CITATIONS

45 C.F.R. § 164.308(a)(2)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE V – SECURITY MANAGEMENT PROCESS

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are REQUIRED by 45 C.F.R. § 164.308(a)(1)

Risk Analysis
Risk Management
Sanction Policy (see Disciplinary Action below)
Information System Activity Review (see Review below)

POLICY

HIE shall ensure that information systems are properly secured and that EPHI is adequately protected. HIE shall implement procedures to prevent, detect, contain, and correct security violations. The components of this policy include:

1. **Risk Analysis –** HIE shall conduct an annual assessment of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of HIE's electronic information which includes, but may not be limited to EPHI.

2. **Risk Management** – HIE shall implement security measures sufficient to reduce risks and vulnerabilities to the Confidentiality, Integrity, and Availability of electronic information (including EPHI) to an appropriate and reasonable level as determined by HIE management.

3. **Disciplinary Action** – HIE shall take appropriate disciplinary actions against HIE Users who knowingly fail to comply with information security-related policies and procedures.

4. **Review** – HIE shall implement procedures to review records of information systems activity to gauge the effectiveness of Administrative, Physical, and Technical safeguards as well as identify possible breaches of information security.

PROCEDURE

1. **Risk Analysis** – At least every **[24 months**], the Security Officer or his/her Designee shall inventory and assess applicable systems/applications. The *Security Controls Questionnaire* (Appendix E) may be used as guidance for ascertaining the security-related features of the system. Specific risks in the areas of data Confidentiality, data Integrity, and systems Availability shall be enumerated along with established safeguards or controls. A conclusion shall be reached as to the reasonableness and adequacy of the existing controls along with corrective measures to be taken. These conclusions and recommendations shall be documented in the risk analysis report and maintained for a period of 6 years. More frequent assessments shall occur prior to all major enhancements, upgrades, conversions, and related changes associated with systems that collect, transmit, manipulate, store, or disseminate EPHI.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

PLEASE NOTE: Appendix E (Security Controls Questionnaire) *is not an all-inclusive questionnaire for assessing risks. It may be used as a guideline in addition to security requirements established by HIE and/or external security personnel for assessing risks.*

2. **Risk Management** – As part of a security management process, HIE shall document and review existing systems and related safeguards to protect their Confidentiality, Integrity, and Availability. As part of such review, HIE shall conduct a risk assessment, including an inventory of systems/applications, related security threats and vulnerabilities, and associated risks. HIE's risk management team shall meet periodically to discuss risk areas and implement updates/controls that are necessary to mitigate identified risks.

   Refer to the following samples for details on identifying/assessing risks in HIE's information technology environment.

   - ***Attachment 1 – Infrastructure Control Matrix;***
   - ***Attachment 2 – Server Control Matrix;***
   - ***Attachment 3 – Application Control Matrix;***
   - ***Attachment 4 – Workstation Control Matrix;***
   - ***Attachment 5 – Disciplinary Action Matrix;***
   - ***Attachment 6 – Risk Analysis Matrix; and***
   - ***Attachment 7 – Auditing/Review Procedures Matrix.***

3. **Disciplinary Action** – In an effort to enforce organizational information security policies, HIE shall establish administrative mechanisms to identify non-compliance. The assigned Security Officer shall maintain records of security incidents/breaches and/or security policy violations. Human resources personnel shall maintain records of disciplinary actions applied to each violation. See **Attachment 5** for samples of disciplinary actions associated with specific violations.

4. **Review** – Based on risks identified, an individual or set of individuals shall determine the sample size, frequency, and data for audit reviews. The Security Officer shall, on a **[quarterly, semi-annual, annual]** basis, review system activity (e.g., login failures, file accesses, security breaches, etc.) and HIE User compliance with security policies. A sample matrix of items to be reviewed is included in **Attachment 7**. Assigned individuals shall periodically discuss audit results, investigate security breaches and determine disciplinary actions, respond to potential weaknesses, assess the security program, develop/amend policies/procedures, and include additional security-related matters.

   If any HIE Users are identified as the source of any security violations based on audits or reports, disciplinary actions shall be enforced. For details on reporting security violations, please refer to the **Security Incidents Policy**.

CITATIONS

45 C.F.R § 164.308(a)(1)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 1

Infrastructure Control Matrix

GOOD PRACTICE

Good Practice	Complete Y/N	Expected Comp. Date	Comments
Cabling in server room and communication closets should be neat and well organized.			
Cable jacks at workstations should be labeled such that cable runs can be traced back to a specific jack in the communications or server room.			
Communications closets that contain hubs, switches, routers, etc. should be locked. Only authorized personnel should have access.			
Communications equipment (hubs, switches, routers, etc.) should be protected by battery backup devices.			
If possible, unused ports on hubs and switches should be disabled.			
Routers and switches should be maintained with up-to-date versions of firmware and any software updates identified by the vendor that patch security vulnerabilities.			
If the local area network is connected to the Internet, a firewall should be in place.			
Devices on an Internet connected local area network should NOT have registered Internet addresses. Network Address Translation and/or proxy should be used.			
All critical servers and workstations should be protected by battery backup devices.			
Servers should be located in a secure (locked) area and only authorized personnel should have access to the server room.			
The room that contains servers should have its own air conditioning and humidity controls as well as adequate fire suppression.			
Backup tapes, when not in use, should be stored in a locked, fireproof (media rated) cabinet or safe.			
Backup tapes or copies (sufficient to restore data and applications in the event of a disaster) should also be stored in a secure, off-site location.			
Backup tapes should be tested quarterly to ensure that data can be restored from backups.			
Vendors working on communications or computer equipment should be supervised. All vendors should execute Confidentiality agreements.			

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 2

Server Control Matrix

GOOD PRACTICE

Good Practice	Complete Y/N	Expected Comp. Date	Comments
All servers should be in a secure, climate controlled room.			
All servers should be protected by battery backup devices.			
All server console screens should be locked or left at a login prompt when not in use.			
Knowledge of Admin User names and Passwords should be limited only to authorized support and management personnel.			
Server operating systems should be kept up-to-date with the latest security patches and maintenance release levels.			
All servers should have software that regularly scans to detect and remove viruses.			
Access control lists (ACLs) for applications and network resources on the server should be regularly reviewed to ensure that only authorized persons have accounts and that privileges are assigned appropriately.			
Modems attached to servers for vendor support should be turned off unless being used by vendor personnel. Vendor personnel should call and request that the modem be activated prior to use.			
Backup copies of server operating system and configuration files should be maintained off-site.			
Guest or "Everyone" accounts should be disabled or at least restricted for access to critical directories and files.			

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 3

Application Control Matrix

(To be completed for ALL applications dealing in any way with EPHI)

GOOD PRACTICE

Good Practice	Complete Y/N	Expected Comp. Date	Comments
Application should require a unique User name and Password for access to the application.			
Application should NOT store User credentials in "clear text" within the application's database.			
There should be written records of authorization to access the application for all Users with access privileges.			
Access levels to the application should be appropriate to the User's role in the organization.			
Access levels should be reviewed quarterly to help ensure only authorized Users have access to the application.			
Users should be required to change their Password periodically. (every 60 to 90 days recommended).			
Knowledge of the administrative or "super User" User name and Password should be limited to only those responsible for system maintenance.			
The application should log access attempts by User.			
Application access logs should be reviewed monthly by an administrator.			
The application should log changes to security settings, and logs should be reviewed at least monthly by an administrator.			
If the application is accessed over the Internet or wireless device, encryption should be enabled for any transmission involving EPHI.			
Regular (daily/nightly) backups should be made of application data, and backups should be stored in a secure, off-site location.			
Original media used to install the application should be kept in a secure location (off-site or media rated safe).			
If possible, application support vendors should be issued a User name (other than generic administrator account) to be used for system maintenance.			
Contact information for support vendors should be maintained by an administrator for use in case emergency support is needed.			

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 4

Workstation Control Matrix

GOOD PRACTICE

Good Practice	Complete Y/N	Expected Comp. Date	Comments
Workstations should have Password protected screen savers or screen blankers enabled after an inactivity period of 5 minutes.			
To the extent possible, workstation screens that contain EPHI should be positioned such that they cannot be viewed by unauthorized Users.			
Critical workstations used in treatment settings should be protected by battery backup units.			
No EPHI should be stored on local workstation drives, only secured shared drives on servers.			
Handheld/palm devices that access EPHI should be Password protected.			
Workstations should be protected by software that actively scans for, detects, and removes viruses.			
Workstation operating system software should be maintained at current release levels and be kept up-to-date with vendor provided security patches.			
Workstations should NOT contain any unauthorized software downloaded or installed by end Users.			
Workstations should NOT contain any application or operating system software that is not legally licensed.			
Workstation usage should be monitored (esp. Internet access), and inappropriate content should be blocked/removed.			

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 5

Disciplinary Action Matrix

GOOD PRACTICE

Level	Violation/Breach	Action/Discipline
I	o Forget to logoff a terminal or lock the computer upon leaving. o Share a User's ID and/or Password o Other	Verbal Warning – The breach is documented and maintained by the Security Officer. The Department Manager is responsible for administering a verbal warning to the User and re-educating the User on policies, procedures, and agreements.
II	o Use another User's ID and/or Password o Allow another User to use your login ID and/or Password o Accessing unauthorized information o Other	Written Warning – Same as the verbal warning but the breach and punishment are documented and signed/acknowledged by the violator. The occurrence is discussed at the Security Committee meeting and a documented report is maintained in the employee's file. Additionally, privileges may be reduced or revoked, depending on the severity of the breach.
III	o Use another's User ID and/or Password o Allow another User to use your login ID and/or Password o Accessing unauthorized information o Disclosure of confidential information	Termination – Documentation of the breach is created, including an explanation of 1st, 2nd, or 3rd violation. Some violations warrant termination on the first occurrence.
IV	o Disclosure of confidential information with intent o Misuse of confidential information with intent o Other	Civil/Criminal suit is brought against the offender. A knowing violation of HIPAA may result in criminal punishment including a fine of up to $250,000 and/or imprisonment for up to ten years. Civil monetary penalties can be assessed under both HIPAA and state law and are capped at $1,500,000 annually.

NOTE: This matrix is only a template of sample violations and associated disciplinary actions. HIE management shall discuss and agree upon levels based on standard operations and legal requirements.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 6

Risk Analysis Matrix

GOOD PRACTICE

*

Threat	Vulnerability	Existing Safeguards	Impact Severity*	Likelihood of Occurrence*	Risk Level*
Environmental/Physical Threats					
Environmental Conditions	Lack of adequate or failure of environmental controls (water leaks, excess humidity, etc.)	Servers are hosted in facility designed to withstand environmental conditions			
Power Fluctuations	Environment is susceptible to power fluctuations	Server facility maintains surge suppressor and backup generator			
Natural Threats					
Natural Disaster / Backup & Recovery	System recovery from backup tapes, databases, and data files is not tested on a periodic basis	All systems are backed up. Full backups occur **[weekly]**; differential backups occur **[daily]**. HIE stores backup tapes at **[local bank]**.			
Natural Disaster / Fire Suppression	LAN rooms not equipped with fire suppression materials	Server facility maintains fire protection over server room			
Human Threats					
Data Entry Errors or Omissions	Entering incorrect values for SSN, financial data, or EPHI could result in data inconsistency	Data is reviewed throughout the collection process			
Inadvertent or Careless Acts	Failure to disable or delete unnecessary HIE User or Participant	Process established to remove access for terminated HIE Users or Participant			

*** Possible Responses include Very Low, Low, Moderate, Significant, and Serious**

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Threat	Vulnerability	Existing Safeguards	Impact Severity*	Likelihood of Occurrence*	Risk Level*
	User accounts could result in unauthorized access to sensitive data Failure to recover terminated employees' key cards and door keys could provide unauthorized access	Users Within 15 minutes of HIE User termination, terminated employee's key card is disabled			
Inadvertent Acts or Carelessness / Omissions	Installation, upgrade, and maintenance errors could leave data unprotected or overly exposed to security vulnerabilities	Servers are patched with each service pack release			
Impersonation	Sharing of badges, key cards, passwords, etc. could provide an unauthorized employee access to EPHI	Employees are instructed not to share badges, key cards, or passwords			
Shoulder Surfing	Monitors are not strategically placed where shoulder surfing is deterred Employees may leave sensitive information unattended on their desks	Physical access to all HIE office space is controlled by electronic key card HIE policy states that all employees should lock their Workstation when unattended Workstations have password-protected screensavers activated after **[10]** minutes of inactivity.			
Theft, Sabotage, Vandalism, or Physical Intrusions	Disgruntled employees could sabotage a computer system by installation of virus software	Background checks performed for all new hires Antivirus software is deployed and is regularly updated			

*** Possible Responses include Very Low, Low, Moderate, Significant, and Serious**

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Threat	Vulnerability	Existing Safeguards	Impact Severity*	Likelihood of Occurrence*	Risk Level*
Technical Threats					
Data contamination	When communicating with outside parties, employees may fail to properly handle EPHI	MS Office encryption is used to send files containing EPHI to outside parties Emails containing EPHI are encrypted			
Corruption by System Errors or Failures	Faulty implementation, such as inconsistency with design or new bugs not covered by specifications could allow compromise of data and application	All system process changes are tested thoroughly before implementation			
Misuse of Known Security Weaknesses	User IDs with weak passwords could allow unauthorized access to EPHI	Password controls include minimum length, expiration, special characters, and password reuse requirements			
Hardware Failure	Hard drives and other components fail on a periodic basis	All systems are backed up; differential backups occur **[daily]**; full backups occur **[weekly]**			
Insertion of Malicious Code or Software	HIE system susceptible to viruses, worms, and Trojans resulting in system damage and data compromise	Antivirus software is implemented on all servers and workstations and is updated often			
Intrusion or Unauthorized System Access	HIE has a susceptibility to unauthorized remote access attempts	HIE perimeter is monitored by an intrusion detection system built into the firewall			

*** Possible Responses include Very Low, Low, Moderate, Significant, and Serious**

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 7

Auditing/Review Procedures Matrix

GOOD PRACTICE

Audit	Description	Frequency
Fax Access	Determine who has electronic faxing capabilities. Only approved Users should be able to free-text fax numbers.	**[Monthly]**
Security Levels	Determine Users with security levels of "ALL" (i.e., super User, access to all functions). Users with ALL access shall be limited.	**[Monthly]**
Logons	Determine the number of concurrent logins for each User. Multiple/concurrent logins allow Users to share IDs more easily, but does not provide accountability. Concurrent logins are easily traced in audit trails.	**[Monthly]**
External Entity	Verify that external access was approved and provided upon a "need to know" basis, depending on type of external entity.	**[Quarterly]**
Segregation of Duties	Ensure that Users do not have dual access to incompatible functions. For example, Users with access to accounts payable shall not have edit access to accounts receivable. Users with access to edit payroll shall not be printing checks.	**[Quarterly]**
Terminated Employees vs. Active Users	Obtain a listing of all active and terminated employees from HR. Extract a system listing of all Users with access. Compare the two lists to identify any Users on the system list who are not on the active/who are on the terminated User list.	**[Quarterly]**
Users Never Logged On	Determine the Users who have never logged on to the system and revoke their access.	**[Quarterly]**
Inactive Accounts (over 30, 60, 90 days)	Determine the Users who have not logged into the system in the past 30, 60, 90 days and evaluate their access needs. For example, sometimes students shall be in the system 3 months and out 3 months.	**[Quarterly]**
Unsuccessful Logon Attempts	Track and report on Users who have attempted to login to the system but have not been able to gain access. Trend duplicate/multiple tries.	**[Daily or Weekly]**
Menus/Functions	Using the Access Control matrix, verify that Users do not have inappropriate access.	**[Quarterly]**
End User Security Policy Agreement	Select a random sample of Users and pull End User Security Policy Agreements for each to determine each User who has **not** signed or click wrapped an access form and/or confidentiality form.	**[Semi-Annually]**
Business Associate Agreement	Select a random sample of Participants and Subcontractors and pull Business Associate Agreements for each to determine which Subcontractors or Participants have not signed or click wrapped a Business Associate Agreement	**[Semi-Annually]**
Walk-Through	Check for screen-savers, visible Passwords (e.g., taped to the bottom of the keyboard, on the screen, etc.)	**[Semi-Annually]**

NOTE: This matrix is only a template of auditing and reviewing frequencies. HIE management shall discuss and agree upon frequencies based on standard operations and legal requirements.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Appendix E

Security Controls Questionnaire

Where appropriate, documentation should be system generated, such as reports, screen shots, or user listings. All information should be provided electronically rather than in hardcopy, unless it only exists in hardcopy. User listings should be provided in text or spreadsheet format, if possible.

GOOD PRACTICE

	Request	Contact	Received
General Requests			
1	Inventory of all systems/applications, including the platform and whether the system contains EPHI. Include server listing (IP, name, O/S, purpose, location).		
2	All policies and procedures related to security. Specifically include the following if available:		
	a. Security Policy - governs the appropriate use of company information systems and data, including EPHI.		
	b. Security Officer – designates a Security Officer and outlines Security Officer's duties		
	c. Security Management Process – outlines the security process		
	d. Workforce Security - includes requirements for authorization, clearance, user notification and termination.		
	e. Information Access Management – contains procedures for access authorization, establishment, and modification and a table of access by job description		
	f. Security Awareness – provides policies for security reminders, protection from Malicious Software, login monitoring and Password protection.		
	g. Security Incident Procedures - includes definition of and response to security incidents.		
	h. Contingency planning – contains procedures for criticality analysis, data backup and recovery, emergency mode operations, testing and revision.		
	i. Evaluation and Audit – govern review of the other policies		
	j. Vendor Contracts and Agreements – evaluates Participant and Subcontractor Business Associate Agreements		
	k. Facility access control - controls and validates individuals' access to facilities based on their role or function, including visitor/contractor control.		
	l. Workstation Use and Security- addresses machines that contain EPHI data and those that do not.		
	m. Device and Media Controls - governs the disposal and/or destruction of EPHI data		
	o. Sanctions – formally defines steps for use when a workforce member fails to comply with security policies and procedures.		

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

	Request	Contact	Received
3	Organization chart.		
4	Job Descriptions.		
5	Security Awareness and Training documentation.		
6	Contingency Plans – including business continuity and disaster recovery.		
7	Log of incidents, if available.		
8	Listing of Business Associates (as defined by HIPAA security standards).		
9	Current Active Employee Listing, including name, department, job title, and date of hire.		
10	Terminated employee listing for employees terminated over the past year. Include name, department, job title, date of hire, and date of termination.		
Network/Infrastructure Requests			
11	Network diagram (include external and internal IP addresses and host info).		
12	Wireless networks - Description and use/purpose.		
13	List of security controls/management processes in place (e.g., regular vulnerability scans, patch management software, log monitoring, etc.).		
14	Copy of any security assessments or audit reports done in the last 2 years.		
15	Network User Listing, including status and password expiration setting.		
16	Network Share access listing.		
17	Network group/member listing.		
18	Evidence of audit trails (settings, recent audit logs) for network activity.		
19	Evidence of Anti-virus and spyware software, including settings for periodic updates and scanning.		
20	Badge Access listing (if applicable) showing associates with access to building and data center/server room.		
21	Description of remote access architecture.		
22	Remote access user listing.		
23	Backup Schedule/Logs.		
For each application containing EPHI, please provide:			
24	User Listing, including user role/access assigned.		
25	Evidence of audit trails (settings, recent audit logs) and evidence that audit trails are reviewed.		
26	Password settings for the application, including expiration and automatic logoff.		
27	Users with access to the database supporting the application.		
28	Password settings for database level users.		
29	Evidence of user reviews.		
Meeting Requests			
30	PHI/EPHI Data Flow (business process walkthroughs).		

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

	Request	Contact	Received
31	Network Security – General overview of processes.		
32	Policy and Procedures – process for reviewing, updating, distribution.		
33	Security Awareness Training.		
34	Business Continuity and Disaster Recovery/Backup Processes.		
35	Business Associate Agreements.		
36	Physical Security over data center/server room and building.		
37	Data Devices – destruction and re-use.		
38	User Access Management – adding, removing, and reviewing users.		
39	Application Development/Programmed Security Controls, including authentication and transaction security.		

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE VI – WORKFORCE SECURITY

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are ADDRESSABLE pursuant to 45 C.F.R. § 164.308(a)(3)

- **Authorization and/or Supervision**
- **Workforce Clearance Procedure**
- **Termination Procedures**

Editor's Note: Reminder that these Model Policies are scalable and addressable. They serve as guidance and can be modified based on the HIE's size, technology and resources.

POLICY

HIE shall ensure that each HIE User has appropriate access to EPHI, based on his/her role within HIE and his/her need to access the data. Controls shall be implemented to prevent individuals who should not have access from obtaining such access. Specific features of HIE's Workforce Security Policy shall include:

1. **Authorization and/or Supervision** – All HIE Users shall be authorized to access systems and applications containing confidential information (including EPHI) ***prior*** to being granted access to those systems. Written records of authorization for systems and application access shall be maintained by the Security Officer for a period of not less than 6 years.

2. **Workforce Clearance Procedures** – An HIE User's access shall be reviewed **[annually]** (after initial authorization) to help ensure that such HIE User's continued access to EPHI is appropriate.

3. **User Notification** – HIE Users shall be notified in writing of their responsibilities related to maintaining the Confidentiality, Integrity, and Availability of EPHI and expected adherence to HIE's information security policies.

4. **Termination Procedures** – Upon termination of, or the end of an arrangement with, an HIE User, adequate steps shall be taken to help ensure the rapid removal of the HIE User's access to facilities and systems that contain EPHI.

PROCEDURE

Prior to HIE Users gaining physical or systems access to any system that contains EPHI, the following conditions shall be met:

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

- Verify that HIE Users requesting access are authorized via the ***System Access Request/Renewal Form***.

  Refer to Attachment 2 in the Information Access Management Policy.

- Validate that all HIE Users, including operating and maintenance personnel, have minimum necessary access (i.e., access is restricted by role/function within the organization).

- Confirm that HIE Users, including technical maintenance personnel, have attended system security awareness training and understand security details (Password maintenance, incident reporting, virus protection, etc.) and security responsibilities for maintaining Confidentiality.

- Require HIE Users to sign an End User Security Policy Agreement acknowledging responsibility for security and Confidentiality of EPHI accessed and/or encountered.

  Refer to Attachment 3 in the **Information Access Management Policy** for a copy of the ***End User Security Policy Agreement.***

- Supervise HIE Users performing technical systems and/or maintenance activities.

Additionally, the Security Officer, or his/her designee, shall maintain ongoing documentation of, and periodically review access levels granted to, each HIE User accessing EPHI. If at any time an HIE User no longer requires or is no longer authorized for access, access shall be changed or removed.

In the event of an HIE User's termination, or in the event of an arrangement with an HIE User who is a volunteer that ends, **[HIE's human resources personnel]** shall notify information technology personnel (or their designee) of the HIE User's last day of employment or work. These procedures are important to prevent the possibility of unauthorized access to secure data by those who are no longer authorized. When an HIE User terminates his or her employment, volunteer, or contractual arrangement with HIE (and hence no longer requires access), department/practice managers shall contact human resources and information systems personnel (or their respective designee). As a detective control, human resources personnel shall also send a listing of all terminated employees/contractors/volunteers to the Security Officer (or other designee) on a **[daily]** basis. Before an HIE User is terminated, human resources personnel or the Security Officer shall coordinate to complete the following items prior to releasing the HIE User's final paycheck.

- Collect portable computers, peripherals, and files;

- Collect keys, tokens, and/or cards that allow physical or system access;

- Remove the HIE User from access lists, including, without limitation, taking any actions necessary to remove the HIE User from the access lists of any Business Associate or Subcontractor systems which contain EPHI;

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

- Remove the HIE User's account(s) from the system(s), including, without limitation, taking any actions necessary to remove the HIE User's account from any systems containing EPHI of Business Associates or Subcontractors; and

- Change locks (e.g., combinations, keys, etc.), if necessary.

See **Information Access Management Policy** for further details regarding access authorization, establishment, and modification.

CITATIONS

45 C.F.R § 164.308(a)(3)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE VII – INFORMATION ACCESS MANAGEMENT

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are REQUIRED by 45 C.F.R. § 164.308(a)(4):

- **Isolating Health Care Clearinghouse Function (NOT APPLICABLE TO HIEs)**

The following implementation specifications are ADDRESSABLE:

- **Access Authorization**
- **Access Establishment and Modification**

Editor's Note: Not all HIE's may have end user documentation. This may vary by HIE. These Model Policies serve as guidance and can be modified based on the HIE's size, technology and resources.

POLICY

HIE shall ensure that access to EPHI is authorized, correctly provided/modified, and removed timely for all Users. Access to EPHI shall be authorized to ensure the Confidentiality, Integrity, and Availability of the information. Specific features of HIE's Information Access Management Policy include:

1. **Authorization** – All Users shall be authorized to access systems/applications containing EPHI ***prior*** to being granted access. Written access authorization records shall be maintained for a minimum of 6 years. With respect to HIE Users, also see the **Workforce Security Policy**.

2. **Access Establishment and Modification** – Written (or electronic) documentation shall be maintained of each User's system access and authorization levels when such access or authorization is granted, reviewed, or modified. This documentation shall be maintained by the Security Officer for a period of not less than 6 years.

PROCEDURE

1. **Authorization** - When access is warranted, HIE's policy is to grant access privileges, both to HIE Users and Participant Users, based on the principle of minimum necessary access, unless an exception to minimum necessary applies by law and in accordance with HIE's policies. The ***Sample Authorization Level Form*** **(Attachment 1)** can be used to designate departmental/individual access to systems. Access shall be requested and authorized via the sample ***System Access Request/Renewal Form*** (**Attachment 2**).

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

2. **<u>Access Establishment and Modification</u>** – Defined roles and base level access privileges are identified in the ***Sample Authorization Level Form***.

A. Establishment

- <u>New HIE Hires</u> – Base levels of system access shall be granted to individuals based on notification from Security Officer and the role identified for the new HIE User. Upon initial setup, departmental management shall request access (beyond base-level access) to systems via the ***System Access Request/Renewal Form***.

- <u>Established HIE Users (who change positions in HIE)</u> – Once an HIE User's base-level access has been established, the Security Officer shall review all requests for systems access beyond a base level for appropriateness. The ***System Access Request/Renewal Form*** contains the systems and functions within those systems available for access. No access shall be granted without the completed and approved form and a signed ***End User Security Policy Agreement*** (**Attachment 3**). Access privileges shall be reviewed annually and shall be formally renewed by the Security Officer (or his or her designee). Annually, the ***System Access Request/Renewal Form*** shall be re-submitted to all department/practice managers to verify the need for continued systems access for each HIE User. Department managers shall have **[5]** working days to respond to these requests for renewal. HIE Users whose access is not renewed shall have their access privileges revoked. HIE Users shall re-sign the ***End User Security Policy Agreement*** annually.

- <u>Non-Employee HIE Users</u> – Non-employed HIE Users (vendors, consultants, contractors, etc.) requiring access to HIE's information systems shall be approved for access by the Security Officer. HIE Users shall sign the ***End User Security Policy Agreement***. All external access privileges shall be granted on the principle of minimum necessary access, and access privileges shall be revoked after the HIE User's need for access is completed. Security Officer shall maintain a listing of non-employee HIE Users with system access privileges, the systems involved, and the dates on which those privileges are granted and revoked.

- <u>Participant Users</u> – Participant Users (hospitals, physicians, etc.) requiring access to HIE's information systems shall be approved for access by the Security Officer. Participant Users shall sign the ***End User Security Policy Agreement*** before being granted access to EPHI. The End User Security Policy Agreement may be signed by click wrap as an alternative to hard copy. All external access privileges shall be granted on the principle of minimum necessary access, unless an exception to minimum necessary applies by law and in accordance with HIE's policies. Access privileges shall be revoked after the Participant User's need for access is completed. Security Officer shall maintain a listing of Participant Users with system access privileges, the

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

systems involved, and the dates on which those privileges are granted and revoked.

B. Modification

- Increased/Additional Access Requests – HIE User shall make a written request to the Security Officer to have additional access privileges granted to an HIE User once initial access has been established based on the HIE User's role and the initial request for access. The Security Officer shall approve and maintain documentation of these requests. The ***System Access Request/Renewal Form*** shall be used to request changes to access privileges. Should a Participant User request additional access, the Participant User's Participant Agreement should be consulted prior to granting additional access privileges.

- Reduction of Access Privileges – If system access privileges must be restricted for reasons other than termination, Security Officer shall notify information technology personnel in writing using the ***System Access Request/Renewal Form***. Requests to Security Officer shall be reviewed and documented for appropriateness and quality control. Should a Participant User request additional access, the Security Officer shall review the Participant User's Participant Agreement for cure periods, appeal rights, notification requirements, etc. prior to reducing access privileges.

C. Termination – In the event of an HIE User's termination, Security Officer shall notify information technology personnel (or their designee) of the HIE User's last day of employment or work. Before an HIE User leaves, HIE HR personnel and/or the HIE Security Officer shall coordinate to obtain physical items such as keys, access cards, computers, and peripherals and remove system access. See the **Workforce Security Policy** for further details. With respect to Participant Users who are terminated, the Security Officer shall review the Participant User's Participant Agreement for cure periods, appeal rights, notification requirements, etc. prior to terminating access privileges.

CITATIONS

45 C.F.R § 164.308(a)(4)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 1
Sample Authorization Level Form

GOOD PRACTICE

HIE USERS					
Department Name	**Read Only**	**Upload**	**Download**	**Edit**	**Delete**
Maintenance					
Security	✓	✓	✓	✓	✓
Business Office	✓				
Human Resources	✓				
Information Systems	✓	✓	✓	✓	✓
Payroll	✓				

PARTICIPANT USERS					
Participant User Type	**Read Only**	**Upload**	**Download**	**Edit**	**Delete**
Hospital	✓	✓	✓		
Physician	✓	✓	✓		
Nurse Practitioner or Physician Assistant	✓	✓	✓		
Pharmacist	✓	✓	✓		
Nurse	✓				
Certified Medication Aide	✓				

Legend:

✓ = Access Provided
[BLANK] = No Access Provided

NOTE: This form is only a template and should be modified based on HIE's system(s). An individual matrix should be completed for each applicable system to ensure "minimum necessary" access.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 2

System Access Request/Renewal Form

GOOD PRACTICE

Requestor Name: _____

Company or Department: _____

Date: _____

System Requested:	User ID Assigned	Expiration	Date Granted	Date Renewed	Date Revoked	Who Administered

Requestor Signature: _____ Date: _____

Security Officer (or designee) Signature: _____ Date: _____

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Attachment 3

End User Security Policy Agreement

GOOD PRACTICE

I, _____, a(n) employee, contractor, Participant, or other affiliated party of HIE, acknowledge that I have been granted access to HIE's information systems resources, including, but not limited to, licensed software, hardware, and data in any form. Security policies apply to all information that is recorded, transmitted, stored, and/or processed electronically by HIE.

I further acknowledge the data contained in, and accessed using, the information systems and network of HIE, and any other automated system that I may use in the course of performing daily responsibilities, shall remain **Confidential**. As a result, I shall not discuss, disclose, modify, provide, or otherwise make available, in whole or in part, such confidential information unless authorized for specific business or clinical purposes.

I agree NOT to share login IDs and/or Passwords with other employees/Users. I also agree that if I must share my login ID/Password for troubleshooting purposes, I must change my Password immediately upon correction of the problem(s).

I understand and agree that all HIE information is to be used for official business only and not for personal use. I understand that HIE reserves the right to monitor, access, and disclose any communications using its systems, and, therefore, I do not have a reasonable expectation of privacy. I also understand that it is my responsibility to protect data and systems from tangible/intangible destruction, viruses, corruption, or anything else that may damage, alter, destroy, corrupt, or make EPHI unusable.

I shall take all precautions to ensure protection, Confidentiality, and security of information and systems. I shall perform my duties with quality and integrity, in a professional manner, and in keeping with established standards. I shall report all violations of security and/or Confidentiality to my supervisor, the HIE Security Officer, or another designee.

I also agree that my obligation is to maintain Confidentiality and security of all information prior to, during, and after termination of any agreement, relationship, and/or employment with HIE. Additionally, I understand that my access to any/all information shall be revoked upon termination or upon authorization by designated individuals.

By signing this agreement, I acknowledge the following: (i) I have read and understand this agreement; (ii) I shall comply with HIE's security policies; (iii) I understand the consequences of violating said policies and this End User Security Policy Agreement, up to and including termination; and (iv) I agree to be bound by applicable security/Confidentiality requirements and contractual obligations. (v) I represent and warrant that any information that I add to the HIE is: (a) current, accurate, and (subject to any restrictions imposed by law or this End User Security Policy Agreement) complete; or (b) if it is incomplete, that the information contains an appropriate indication to that effect; and (c) complies with any requirements of HIE's policies and procedures as to format or content.

_____	_____	_____
Name	Signature	Date

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE VIII – SECURITY AWARENESS

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are ADDRESSABLE pursuant to 45 C.F.R. § 164.308(a)(5):

- **Security Reminders**
- **Protection from Malicious Software**
- **Login Monitoring**
- **Password Management**

NOTE: The training required pursuant to this Section is IN ADDITION TO the workforce role-based training requirements contained in Section 181 of the Texas Health and Safety Code, as added pursuant to House Bill 300, 82nd Legislative Session, and set forth in Article XII of the Model Privacy Policies.

POLICY

HIE shall ensure that all HIE Users are educated on security risks and accountability regarding properly securing EPHI. HIE shall provide periodic security awareness and training to all HIE Users (including management). Specific features of the awareness and training policy shall include, but may not be limited to:

1. **Security Reminders** – Periodic communications on information security policies and procedures.

2. **Protection from Malicious Software** – Training on procedures to protect against, detect, and report malicious software such as viruses.

3. **Login Monitoring** – Training on how to identify (if possible) unauthorized use of access credentials by an unauthorized party.

4. **Password Management** – Training on how to create, change, and safeguard Passwords.

PROCEDURE

1. **Security Reminders** – All HIE Users, including management, shall receive initial awareness training to gain a better understanding of security policies and procedures. **[Title]** shall be responsible for educating HIE Users on the Physical, Technical, and Administrative security safeguards. Training shall include, among other things, risk areas, access granting and revocation procedures, access levels, Password management, virus protection, identifying and reporting security breaches, and associated disciplinary procedures. In addition to initial training, periodic security reminders shall be distributed via mail, e-mail, flyers, etc.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

2. **Virus Protection** – Designated individuals shall also discuss malicious attacks on HIE's systems, including various types of viruses. In addition, steps for identifying, reporting, and preventing viruses shall be communicated. HIE shall implement antivirus software that periodically scans and updates servers and workstations with the most recent virus definitions.

3. **Login Monitoring** – As part of HIE's auditing procedures, HIE shall review all failed login attempts (e.g., time, number of attempts, ID, etc.) and successful logins (e.g., information accessed – by exception only, ID, time logged in, etc.). HIE also shall have procedures in place for reporting and handling discrepancies and unauthorized activity.

4. **Password Management** – User IDs shall uniquely identify specific individuals to provide HIE User accountability (via logs) and help prevent unauthorized access.

   Passwords are required and shall include at least **[enter length requirement] [specify alpha, numeric, and/or special characters]** characters. Users shall be instructed to choose Passwords that are difficult to guess. Some "**Do**" and "**Don't**" suggestions regarding Passwords are as follows:

   Do (easy to remember but harder to guess)

   (a) String several words together (the resulting Passwords are also known as "pass phrases");

   (b) Shift a word up, down, left, or right one row on the keyboard;

   (c) Combine punctuation or numbers with a regular word; or

   (d) Create acronyms from words in a song, a poem, or another known sequence of words.

   Do Not (easy to guess; Users should not use)

   (a) Use a Password the same as your User ID;

   (b) Use simple, dictionary words, such as system, admin, department name;

   (c) Use names of children, pets, or loved ones; or

   (d) Use birth dates, social security numbers, addresses, etc.

   Passwords shall not be shared or written down in a place where unauthorized persons might discover them. Sharing Passwords exposes the assigned/responsible User to results of inappropriate actions taken with the disclosed Password. If a User believes that his or her Password has been compromised, the User shall inform HIE's Security Officer to initiate an immediate change.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

CITATIONS

45 C.F.R § 164.308 (a)(5)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE IX – SECURITY INCIDENTS

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are REQUIRED by 45 C.F.R. § 164.308(a)(6):

- **Response and Reporting**

POLICY

HIE shall address attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. HIE shall maintain security procedures to preserve the confidentiality and Integrity of EPHI. HIE's policies shall contain provisions to help prevent detect, contain, and correct various security breaches/incidents.

Response and Reporting – Procedures shall be maintained for individuals to report actual or suspected security incidents to the Security Official. The Security Official shall respond to the incident as appropriate and as directed by management in an effort to mitigate any harmful effects of the incident. The Security Official shall maintain documentation of all security incidents and outcomes for a period of 6 years or based on applicable regulatory requirements (whichever is greater).

PROCEDURE

In the event of a security breach, see the Breach Notification Policy and/or the Sensitive Personal Information Breach Notification Policy contained in the Model Privacy Policies.

A security *breach* means the acquisition, access, use, or disclosure of EPHI in a manner not permitted under the Privacy Standards or Security Standards that pose a significant risk of financial, reputational, or other harm to the individual.

As such, the following steps shall be taken by **[Title]** in the event of a security incident. **[Define procedures as to those responsible for completing these tasks and steps to take to do so.]**

- If possible, stop the incident or the access point in which the incident is occurring.
- Determine the cause and an associated solution to prevent future occurrence.
- Log all incidents, including, but not limited to, type of incident, details, action taken, etc. Use the ***Incident Reporting Form*** (**Attachment 1**).

To report a potential security breach, complete the ***Security Breach Reporting Form*** (**Attachment 2**), and deliver it to **[Location/Title]**. The Security Officer (or his or her designee)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

shall review all security breaches and take appropriate action according to the incident level, as indicated in the ***Sanction/Disciplinary Action Matrix*** (see **Security Management Policy**).

CITATIONS

45 C.F.R § 164.308 (a)(6)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 1

Sample Incident Reporting Form

GOOD PRACTICE

Name: _____ Department: _____

Date Reported: _____ Type of Incident: _____

Description:

_____

_____

_____

_____

_____

Action Taken:

_____

_____

_____

_____

_____

Resolution:

- o Escalated
- o Open
- o Closed

Date Resolved: _____

By whom: _____

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE X – CONTINGENCY PLANNING

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are REQUIRED by 45 C.F.R. § 164.308(a)(7):

- **Data Backup Plan**
- **Disaster Recovery Plan**
- **Emergency Mode Operation Plan**

The following implementation specifications are ADDRESSABLE:

- **Testing and Revision Procedure**
- **Applications and Data Criticality Analysis**

POLICY

HIE shall ensure that information systems containing EPHI and related daily processing can be recovered following an unplanned event. HIE shall maintain policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems containing EPHI. The specific features of this Contingency Planning Policy include:

1. **Applications and Data Criticality Analysis** – Assessment of the relative criticality of specific applications and data in support of contingency plan components;

2. **Data Backup Plan** – Procedures to create and maintain retrievable exact copies of EPHI;

3. **Disaster Recovery Plan** – Procedures to restore any loss of data;

4. **Emergency Mode Operations Plan** – Procedures to enable continuation of critical business processes for the protection of the security of EPHI while operating in an emergency mode; and

5. **Testing and Revision** – Procedures for **[periodic**] testing and revision of contingency plans.

PROCEDURE

HIE assets are infrastructure that contains, maintains, or transmits EPHI. To develop a contingency plan, HIE shall identify and inventory HIE assets including:

- ***Infrastructure Components*** such as hubs, switches, routers, circuits, etc.;
- ***Servers*;**

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

- ***Workstations;***
- ***Applications*; and/or**
- ***Mobile Devices*.**

1. **Applications and Data Criticality Analysis –** As part of identifying HIE's information technology assets, HIE shall determine significant applications, data, and business processes to help document and maintain consistent procedures for recovery in the event of temporary system downtime or extensive system loss. HIE shall complete the following:

- Determine criticality of business processes and associated data/ applications. Refer to the ***Application Criticality*** and ***Data Criticality*** tables in **Attachments 1** and **2**, respectively.
- Analyze identified assets' recovery priority and time objective after an unplanned event;
- Identify threats/vulnerabilities to all information technology assets along with procedures to mitigate and safeguard against threats, based on probability of occurrence and cost/feasibility of implementation;
- Ensure access to HIE's most critical systems and services during an emergency;
- Develop plans to transfer data to other servers, which meet the requirements of this policy and applicable laws and regulations, located in different regions, in advance of a foreseeable disaster to prevent an interruption of service; and
- Complete and document security testing and change control procedures.

2. **Data Backup Plan**

(a) Data on each server shall be backed up and accessible – HIE shall ensure that all critical information on each server has redundant copies stored in different servers, or other appropriate backup methods, at any time. HIEs **[shall endeavor]** to maintain servers in different geographic regions to prevent localized emergencies from disrupting service.

b. Data shall be backed up for long-term storage in case of disaster – HIE shall create **[daily]** long-term backups on all new information on durable media that are disconnected from any network. HIE shall store these long-term backups in a safe that protects them from unauthorized access, fire, water/humidity, changes in environment, and any outside force that could cause their premature deterioration. HIEs [**shall endeavor]** to maintain the long-term backup copies of data offsite, to prevent them from being destroyed in a common disaster.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

c. Data may be backed up by vendors or on cloud servers – HIE **[may]** use a vendor to outsource data backup so long as the vendor complies with all applicable laws, regulations, and policies. HIE cannot delegate liability for security or privacy breaches and is ultimately responsible for the conduct of its vendors. HIE shall not merely rely on the representations of vendors without verifying their data backup procedures and contractually obligating them to meet all legal requirements in a Subcontractor Business Associate Agreement. HIE **[may]** store data in cloud servers so long as the cloud servers comply with all applicable laws, regulations, and policies. HIE cannot delegate liability for security or privacy breaches. HIE shall contractually obligate cloud computing services vendors by a Subcontractor Business Associate Agreement which obligates such vendors to meet all legal requirements, and HIE shall verify that such vendors' procedures in fact do comply with HIE's policies. HIE **[may]**, in its reasonable business judgment, use any process or media so long as such process or media complies with all applicable laws, regulations, and policies, and is considered among the best practices of the information technology industry. All data stored in the cloud shall be Encrypted. HIE shall maintain backups of all patient data **[for at least for the retention period mandated by Texas law for each patient]**.

3. **Disaster Recovery Plan/Emergency Mode Operation** – Access controls shall be in place to enable HIE to continue to operate and/or recover lost data in the event of fire, vandalism, natural disaster, or system failure. HIE shall document plans which include all necessary information to continue processing following system downtime or a loss of data. Plans shall be maintained at HIE's facility and at the offices of all Participant Users. Teams shall be assigned, and HIE shall complete initial and periodic testing of the plans. HIE disaster plans shall ensure that critical services remain operational even during and after a disaster. To view a copy of the plans and/or testing results, contact the Security Official. HIE **[should endeavor]** to maintain redundant servers or data systems in multiple geographic regions to prevent interruptions in service. HIE shall stay abreast of developments in the information technology industry that provide for increased data security and implement any best practices that comply with all applicable laws, regulations, and policies.

4. **Testing and Revision** – Security testing shall be performed periodically to help ensure physical and systems security, as well as compliance with/adequacy of the application's intended purpose. Testing procedures shall include functional testing, penetration/vulnerability testing, and verification. HIE's EPHI shall be protected by intrusion detection systems, such as a firewall. Additionally, periodic audits (e.g., firewall logs and unsuccessful login attempts) shall be reviewed for potential security violations and/or threats.

CITATIONS

45 C.F.R § 164.308(a)(7)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 1

Sample Application Criticality Form

GOOD PRACTICE

Application Name	Vendor/Developer	Version	Usage	Key Support Contact/Phone	Host Name	Install Media Location	Criticality

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 2

Sample Data Criticality Form

GOOD PRACTICE

Database Name	Vendor/ Developer	Version	PHI Data Elements	Key Support Contact/Phone	Host Name	Install Media Location	Criticality

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XI – EVALUATION AND AUDIT

IMPLEMENTATION SPECIFICATIONS

This standard is REQUIRED by 45 C.F.R. § 164.308(a)(8)

POLICY

HIE shall assure the Confidentiality, Availability, and Integrity of EPHI. HIE shall perform a periodic technical and nontechnical evaluation to ensure that HIE policies comply with laws, rules, and regulations. This periodic technical and nontechnical evaluation shall also respond to environmental or operational changes affecting the security of EPHI. The technical evaluation shall include testing and investigation of HIE's technical security procedures, including the algorithms or processes used for Encryption, Authentication, and Integrity. The nontechnical evaluation shall include testing and investigation of HIE's administrative and physical security policies. The Security Officer shall review the effectiveness of existing policies as well as HIE User's and Participant User's compliance with these policies.

PROCEDURE

(a) Inventory of systems and applications – Annually, information systems personnel shall inventory and assess applicable systems/applications. **Attachment 1** provides a recommended evaluation checklist that may be used as guidance for completing the review process but may not be the only requirement for evaluation. HIE shall review existing systems at least annually or upon any major release/upgrade or operational/ environmental changes (i.e., any changes affecting EPHI security) by the Security Official or his or her designee. HIE shall ensure that Subcontractor Business Associate Agreements address this requirement by conducting audits onsite, requiring periodic completion of a security questionnaire, etc.

(b) Technical evaluation – HIE shall ensure that all patches, updates, upgrades, releases, etc. of HIE's systems are tested prior to implementation. HIE shall monitor official publications and warnings from hardware and software companies (e.g. Apple, Microsoft, Oracle) as well as traditional and nontraditional industry publications, conferences, and security forums (e.g. *IEEE Security and Technology*, *Advances in Cryptography*, and DEF CON) and stay abreast of potential threats to EPHI (e.g. malicious software, exploits, etc.). HIE shall review new or proposed systems, upgrades, and updates prior to implementation by the Security Official or his or her designee. The Security Official or his or her designee shall evaluate the potential risks and benefits of each change as compared to the potential risks and benefits of not making a change and shall make a reasoned decision as to what course of action best promotes secure and appropriate access to EPHI for Users. Security Officer shall review audit trails of Users for suspicious activity.

(c) Nontechnical evaluation – HIE may audit Business Associate Agreements and Subcontractor Business Associate Agreements for compliance with current laws, rules, regulations and policies. Security Officer shall inspect the physical security of HIE's facility.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Security Officer shall evaluate compliance with HIE physical's and administrative security policies, such as the issuance of badges and the complete destruction of EPHI-containing devices prior to their disposal. Security Officer may solicit information on the physical security of Participant Users and their compliance with the Physical, Technical, and Administrative Safeguards in the Business Associate Agreements. HIE shall review such information and take action to improve EPHI security.

(d) Record of Review – Upon completion of the evaluations, the results of these evaluations and a record of the Security Official's decision shall be maintained by the Security Official for a period of no less than 6 years. HIE shall continuously monitor the system and shall conduct User audits to discover and address attempted and successful security breaches quickly.

CITATIONS

45 C.F.R § 164.308(a)(8)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 1

Recommended Evaluation Checklist

GOOD PRACTICE

Recommended Evaluation Checklist						
-	**LAN/ WAN**	**E-mail**	***<Custom Application>***	***<Custom Application>***	***<Vendor Application>***	***<Vendor Application>***
Access Controls:						
One of the following: a. Context-based b. Role-based c. User-based						
Procedures for emergency access?						
Does the system use encryption to protect data stored and/or transmitted?						
Audit Controls:						
Does the system have audit trails available?						
Are audit trails activated and monitored?						
Is there a monitoring procedure?						
Are results of audits documented and/or maintained?						
Does the system flag abnormalities or issue an alert signifying suspect activities?						
Authorization Controls:						
Are authorizations confirmed before allowing access to the system?						
Are authorizations User-based or role-based?						
Data Authentication:						
Is data Integrity verified before issue/ acceptance (i.e., verify that the data sent is the data received)?						
Do you employ one of the following data corroboration techniques? 1. Check Sum 2. Double-Keying 3. Message Authentication Code 4. Digital Signature 5. Other						
Entity Authentication:						

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Recommended Evaluation Checklist						
-	**LAN/ WAN**	**E-mail**	***<Custom Application>***	***<Custom Application>***	***<Vendor Application>***	***<Vendor Application>***
Is the entity accessing information from the system verified/validated prior to access?						
Is automatic logoff activated (i.e., the system auto logs off after a period of inactivity)?						
Is unique User identification employed/maintained?						
Do you employ one of the following techniques? 1. Biometrics 2. Passwords 3. Personal Identification Number 4. Callback 5. Token that uses physical device for authentication 6. Other						
Network Controls						
Is the system considered an, or implemented on, an "open network" (i.e., Internet)						
If the system is used via an open network, do you have encryption to help protect information?						
Do you have procedures for the following techniques? 1. Integrity Controls (verify the data has not been altered) 2. Message Authentication (ensure the message is coming from the original sender, that the content has not been changed, and/or the receiver is the one intended)						
Do you have standard procedures for at least one of the following techniques? 1. Access Controls 2. Encryption						
If you transmit information via the network, do you have the following features in place? 1. Alarm (identifies abnormal access/processes) 2. Audit Trails 3. Event Reporting (indicates operational problems with physical elements of the network) 4. Other						

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XII – VENDOR CONTRACTS AND AGREEMENTS

IMPLEMENTATION SPECIFICATIONS

The following implementation specification is REQUIRED by 45 C.F.R. § 164.308(b)(1):

- **Written Contract or Other Arrangement**

POLICY

HIE is a Business Associate of its Participant Users who are Covered Entities. As such, HIE must enter into a Business Associate Agreement with each of its Participant Users. HIE shall not receive any EPHI from a Participant User or Subcontractor until a fully executed Business Associate Agreement has been entered into between the parties. Additionally, HIE shall enter into a Business Associate Subcontractor Agreement with any entity that receives EPHI from HIE and performs a function on behalf of the HIE.

PROCEDURE

Please see the model Business Associate Agreement Policy contained in the Model Privacy Policies.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XIII – HIE FACILITY ACCESS CONTROL

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are ADDRESSABLE pursuant to 45 C.F.R. § 164.312(a)(1):

- **Contingency Operations**
- **Facility Security Plan**
- **Access Control and Validation Procedures**
- **Maintenance Records**

POLICY

HIE shall establish physical access controls (i.e., keys, locks, and cards) to help prevent/detect intrusion/unauthorized access and to ensure that HIE Users have minimum necessary access to perform their daily job functions. Additionally, physical access controls are in place to protect physical computer systems and related buildings in the event of natural disasters and environmental hazards.

HIE shall limit physical access to its electronic information systems and the facilities in which such systems are housed while ensuring that properly authorized access is allowed. The specific features of HIE's Access Control policy include:

1. **Contingency Operations** – Procedures shall allow for system access in support of restoration of lost data under the disaster recovery and emergency mode operations plans in an emergency.

2. **HIE Facility Security Plan** – Safeguards shall be in place to protect the system and the equipment therein from unauthorized physical access, tampering, and theft.

3. **Access Control and Validation Procedures** – Safeguards shall be in place to validate a person's access to facilities based on his or her role or function.

4. **Maintenance Records** – Documentation shall be maintained with respect to repairs and modifications to the physical components of the systems that relate to security.

PROCEDURE

1. **Contingency Operations** – Access controls shall be in place to enable HIE to continue to operate and/or to recover lost data in the event of fire, vandalism, natural disaster, or system failure. HIE shall document plans which shall include all necessary information to continue processing data. Plans shall be maintained electronically and on paper by the Security Officer. Teams shall be assigned, and HIE shall complete initial and periodic

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

testing of the plans. To view a copy of the plan and/or testing results, contact the Security Officer.

2. **HIE Security Plan** – HIE shall document a plan and, as necessary, install **[security alarm system, video monitors, etc.]** to protect and to observe the building(s) (exterior and interior) and surrounding areas from unauthorized physical access. Additionally, HIE shall implement locks and security codes in restricted areas to safeguard information systems equipment from unauthorized physical access, tampering, and theft. Prior to gaining physical access to the building, a person shall sign in at the front desk and be issued a security badge. For all on-employees requiring access to equipment or other sensitive information, the Security Officer, or designee, shall verify the need for access and document arrival/departure and need (e.g., maintenance) of such non-employee. Refer to **Attachment 1** for a ***Sample HIE Security Plan***.

3. **Access Control and Validation Procedure** – HIE shall establish secure areas and limit access to HIE Users who need to work in those areas. The Security Officer shall implement, and periodically review, security procedures, such as badges, keys, increasing zones of security, identity checks, unique pin codes for numeric lock pads, sign-in and sign-out sheets, etc. to reduce the risk of unauthorized access to secure areas. The Security Officer shall ensure that no materials, including photocopiers, that store EPHI are left unencrypted in unsecure areas.

4. **Maintenance Records** – HIE shall maintain logs of all needed repairs to HIE'S facility. Security Officer or Security Officer's designee shall validate the identities of all incoming maintenance staff and confirm that they are authorized to perform required, requested maintenance. HIE shall coordinate with building managers to ensure that environmental conditions in the building such as humidity or temperature do not endanger the media and devices on which EPHI is stored. HIE shall keep a log of all scheduled maintenance, the date on which it is to be and was performed, and the individuals and companies that performed the maintenance. Security Officer shall keep an inventory of all keys and tokens and an Encrypted log of all Passwords and User IDs.

CITATIONS

45 C.F.R § 164.310 (a)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

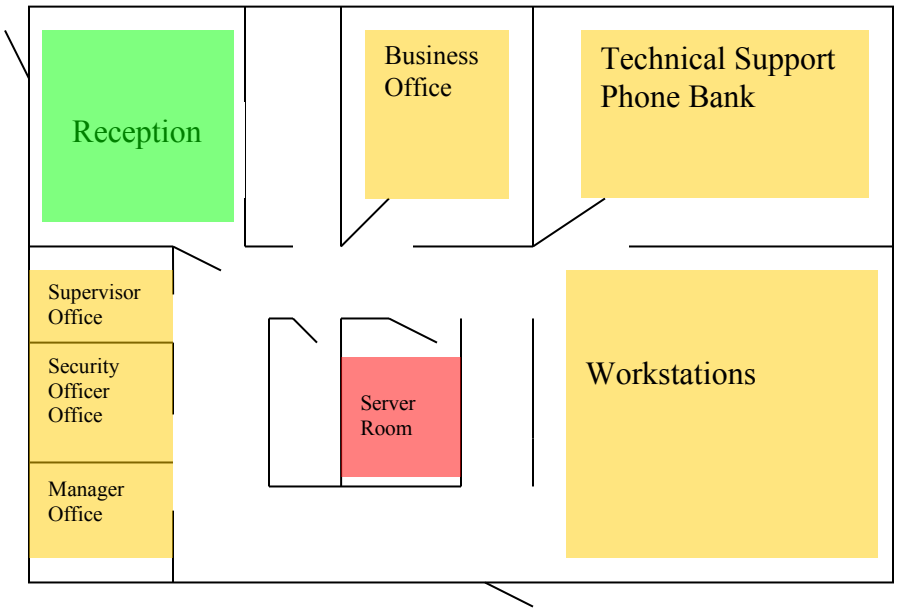
Attachment 1

Sample HIE Security Plan

GOOD PRACTICE

Insert floor plan/diagram for HIE that indicates:

1. Entrances
2. Exits
3. Public Areas (Green)
4. Controlled Access Areas (Yellow)
5. Secure Areas (Red)



In narrative form, describe the access control methods for each area and entrance exit. Include the type of lock (i.e. key, card, combination, etc.), the hours that public areas are open, who maintains keys, and who is allowed in each area. Additionally, include information on alarms, monitoring systems, and other physical security controls.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

Attachment 2

Physical Access Control Summary Worksheet

GOOD PRACTICE

Area	Control Type	Open Access Hours	Restricted to	Control Vendor	Emergency Contact
FOR EXAMPLE ONLY					
Reception Area	*Key Lock/Alarm*	*9 am to 5 pm*	*N/A*	*Lock Vendor Alarm Company*	*Name, phone number*
Business Office	*Key Lock*	*9 am to 5 pm*	*Practice Personnel*	*Lock Vendor*	*Name, phone number*
IT / Server Room	*Combination Lock*	*None*	*IT Staff, Security Officer*	*Lock Vendor*	*Name, phone number*

Building Manager _____
Emergency Contact _____ Phone/Cell/Pager _____
HVAC Vendor _____ Phone/Cell/Pager _____
Alarm Vendor _____ Phone/Cell/Pager _____
Natural Gas Utility Phone _____
Water Utility Phone _____
Electrical Utility Phone _____
Generator/Emergency Power Vendor _____ Phone _____
Waste Disposal Vendor _____ Phone _____

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 3

Security Maintenance Log

GOOD PRACTICE

Whenever changes, additions, or repairs are made to physical access controls such as locks, doors, alarm systems, etc., those activities must be logged. These logs should be maintained for a period of six years.

Item	Description	Date Started/Date Completed	Vendor	Maintenance Personnel Name
FOR EXAMPLE ONLY				
Front Door Key Lock	*Lock changed/re keyed after termination of User*	*Date/Date*	*Lock Vendor*	*Name*
Rear Door Key Lock	*Lock changed/re keyed after termination of User*	*Date/Date*	*Lock Vendor*	*Name*

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XIV – WORKSTATION USE AND SECURITY

IMPLEMENTATION SPECIFICATIONS

This standard is REQUIRED by 45 C.F.R. § 164.310(b)-(c)

POLICY

HIE shall ensure that all HIE User workstations are properly secured to help mitigate the risk of unauthorized access to information. HIE shall implement, and shall educate Participant Users on implementing, procedures regarding physical safeguards over workstations, especially those located in less secure/public areas. HIE shall define acceptable uses for HIE User workstations. Additionally, HIE shall implement physical security controls to properly secure HIE User workstations.

PROCEDURE

Workstations shall be used solely for conducting HIE business. All personal use, including installation of personal software, shall be prohibited. Workstations shall be used only to access the applications for which the logged-on User is authorized.

1. **Workstation Use** – While working on-site or remotely, HIE Users shall take every precaution to operate systems and process data securely and confidentially. Consequently, information obtained via HIE's or an affiliate's systems shall not be taken off-site or shared with anyone without prior approval from the Security Officer or his or her designee. Processing and/or transmission shall employ proper controls to maintain data Integrity and system Availability.

   No HIE User shall be permitted to modify hardware or software configurations or copy/transport software for personal use without prior approval from the Security Officer or his or her designee.

   E-mail and voicemail services for HIE Users shall be the property of HIE. Consequently, HIE Users shall have no reasonable expectation of privacy. These privileges shall be used according to specific guidelines located in the **[policy, manual, or other location name]**.

   Use of the Internet shall be limited to business use only. Internet activity shall be logged, and inappropriate use shall be handled accordingly

2. **Workstation Security** – Workstations/terminals shall be set up so that only authorized Users can view EPHI. Unattended workstations left unsecured may promote intentional and/or accidental breach of Confidentiality and security, thereby leaving the last person logged in accountable for actions taken. HIE shall implement the following procedures

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

with respect to HIE User Workstations and shall educate Participant Users on securing Participant User Workstations according to the following:

- Workstations with access to EPHI shall be secured such that unauthorized parties may not gain access to protected or confidential HIE information and EPHI. When practical, such workstations shall be located in areas not accessible to the public.

- Workstations with access to EPHI in public areas shall never be left in a "logged on" state while unattended. Workstations, regardless of location, with access to EPHI shall not be left unattended for more than **[5]** minutes without the current User logging off of the application and/or network or engaging a screen saver that requires a Password for access. In other words, every User shall implement a Password-protected screen-saver.

- Unattended terminals shall be automatically logged off after a period of inactivity. If auto-lockout is not enabled on the terminal, Users shall log off before leaving a terminal unattended to help maintain physical security.

CITATIONS

45 C.F.R § 164.310 (b-c)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XV – DEVICE AND MEDIA CONTROLS

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are REQUIRED by 45 C.F.R. § 164.310(d)(1):

- **Disposal**
- **Media Re-use**

The following implementation specifications are ADDRESSABLE:

- **Accountability**
- **Data Backup and Storage**

POLICY

HIE shall ensure that portable information systems are protected from unauthorized access and release. Unencrypted computing devices (e.g. PCs, laptops, PDAs, servers, smart phones, other mobile phones, tablets, digital e-readers, photo copiers, etc.) and electronic storage media (e.g. hard drives, solid state drives, floppy disks, CDs, DVDs, backup tapes, external removable storage devices, flash drives, SD cards, SIM cards, etc.) that contain EPHI or other confidential data shall be tracked as they move into and out of HIE's facilities.

HIE shall maintain a log, for example, by using RFID technology and/or the device's location tracking applications, of all devices and media that come into contact with EPHI, that includes when the device or media first encountered EPHI, where the device is physically located, if it has been moved within the facility, and if and when the device or media has been thoroughly and appropriately cleaned of EPHI and/or transported outside of the HIEs control.

HIE shall report the loss of any device or media potentially containing EPHI immediately to the covered entities with which they interact. HIE shall isolate EPHI-containing devices and media from non-EPHI-containing devices and media. HIE shall remove EPHI from devices and media in accordance with National Institute of Standards and Technology (NIST) standards.

PROCEDURE

Specific features of this Device and Media Control policy include:

1. **Use.** HIE shall ensure that all devices and media are Encrypted in accordance with NIST standards. All workstations not located in secure locations that will be used to access and/or store EPHI shall be fully Encrypted. Workstations in secure locations need not be fully Encrypted, but all EPHI accessed or stored therein shall be Encrypted. Flash drives and other portable storage media shall be fully encrypted.

2. **Disposal** – Personnel needing to dispose of electronic devices or media shall contact the Security Officer. The Security Officer's designee shall remove EPHI data and/or dispose of hardware appropriately and in accordance with NIST standards to help prevent

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

unauthorized access/dissemination of EPHI. Prior to disposing of a device or media that contains EPHI, HIE must remove all EPHI data from the media. HIE must use its judgment and NIST standards to ensure it has removed all EPHI from the media and prevented any possibility of recovery of EPHI. Where possible, HIE shall use a combination of physical and software based removal methods. When a device or media will not be reused and prior to its disposal, HIE shall physically destroy or render the device inoperable and irreparable.

3. **Reuse** – If a device or media is to be reused by other parties without authorization to access the EPHI located on the device or media, HIE must remove all EPHI data from the media. Data removal must meet or exceed the NIST standards. HIE must use its judgment and industry best practices to ensure that it has removed all EPHI from the device or media and prevented any possibility of recovery of EPHI by an unauthorized user.

4. **Accountability** – All devices and media that have at any point contained or processed EPHI shall be identified with a unique identifier. HIE shall maintain a log of all devices and media that come into contact with EPHI that includes when the device or media first encountered EPHI, where the device is physically located, and if and when the device or media has been thoroughly and appropriately cleaned of EPHI and/or transported outside of HIEs control. If devices or media are to be sold or donated, the Security Officer shall be responsible for maintaining a record of movement for the media, identifying the date, new location, and the individual responsible for the movement of the device/media, along with the new end-user of the device or media if applicable. HIE shall report the loss of any device or media potentially containing EPHI immediately to the covered entities with which they interact. HIE shall isolate EPHI-containing devices and media from non-EPHI devices and media. See **Attachment 1** (***Media Controls Form)***.

5. **Data Backup and Storage** – HIE shall make backups of EPHI prior to movement of equipment when loss of availability of the data poses a risk to HIE or the patients whose information HIE accesses. Details regarding backups, such as frequency, storage, etc., can be found in the ***Contingency Planning Policy***.

CITATIONS

45 C.F.R § 164.310 (d)

NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*

NIST, *HIPAA Security Rule Toolkit User Guide*

NIST SP 800-92, *Guide to Computer Security Log Management*

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

[Name of HIE]

Attachment 1

Sample Media Controls Form

GOOD PRACTICE

Name:_____ Department:_____

Hire Date:_____ Term Date:_____

Checkout Date:_____ Check-In Date:_____

Hardware o Laptop o PDA o Security Cable o Modem o CD Burner o Disk Drive o Hub o USB drive o Portable hard drive	Access Tools o ID Badge o Keys o Security Access Card o Token o Secure ID o Other
Other o Software o Company Credit Card o Cell Phone o Company Policies/Documentation	

Note/Serial Numbers

_____

_____

Employee Signature: _____ Date: _____

Security Officer Signature: _____ Date: _____

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XVI – TECHNICAL ACCESS CONTROLS

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are REQUIRED by 45 C.F.R. § 164.312(a)(1):

- **Unique User Identification**
- **Emergency Access Procedure**

The following implementation specifications are ADDRESSABLE:

- **Automatic Logoff**
- **Encryption and Decryption**

POLICY

HIE shall ensure that access to information systems is properly controlled and restricted to authorized individuals. HIE shall implement Technical Safeguards for electronic information systems that maintain EPHI to allow access only to those programs and persons that have been granted access rights according to access control and authorization policies. The specific features of the Access Control Policy include:

1. **Unique User Identification** – Unique user IDs and Passwords shall be assigned to each User.

2. **Emergency Access Procedures** – Procedures shall ensure access to EPHI in an emergency.

3. **Automatic Logoff** – Unattended workstations/terminals shall be locked down following a period of inactivity.

4. **Encryption/Decryption** – Preference shall be given in system selection to applications and operating systems that allow for the encryption of User credentials and EPHI. Encryption, if used, shall be accomplished using standard (non-proprietary) algorithms.

PROCEDURE

1. **Unique User Identification** – An HIE User's access to HIE's systems, resources, and/or health information shall be granted only after approval and on a "minimum necessary" basis, unless an exception to minimum necessary applies by law and pursuant to HIE's policies. Each HIE User shall have a unique identifier (no shared IDs) to gain access and provide accountability. Default file permissions (read, write, or execute) shall only be provided to authorized HIE Users. HIE Users shall implement Password-protected screen savers to prevent unauthorized access to their machine(s).

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

2. **Emergency Access Procedures** – If an HIE User requires access to EPHI outside of his/her daily job function, access shall be authorized by the department manager and Security Officer. If access must be provided prior to approval, access and activity shall be logged and approved following the access/activity. Procedures for accessing critical systems containing EPHI during an emergency shall be detailed in the emergency mode operations plan.

3. **Automatic Logoff** – Networked workstations in an unsecured area with access to EPHI shall be configured to lock and blank the screen after **[10]** minutes of inactivity. Networked workstations in secured areas with access to EPHI shall be configured to lock and blank the screen after **[30]** minutes of inactivity. A user ID and Password shall be required to unlock each workstation. Stand-alone workstations shall be configured utilizing a locking screen saver after **[10]** minutes of inactivity. HIE shall implement automated procedures to terminate a remote electronic terminal session after **[10]** minutes of inactivity.

4. **Encryption and decryption** – EPHI transmitted/received via e-mail and/or other non-secured means shall be encrypted/decrypted via the **[encryption method]** encryption system established by HIE's information technology department. Please contact the Security Officer for details on activating and using these services. Refer to **Transmission Security – Encryption Policy**.

5. **Participant Users** – Prior to Participant Users gaining remote access to HIE's systems, the following conditions shall be met:

   - Validate that all Participant Users have minimum necessary access, unless an exception to minimum necessary applies by law and pursuant to HIE's policies.

   - Confirm that Participating Users have attended system security awareness training and understand security details (Password maintenance, incident reporting, virus protection, etc.) and security responsibilities for maintaining Confidentiality.

   - Require Participant Users to sign an End User Security Policy Agreement acknowledging responsibility for security and Confidentiality of EPHI accessed and/or encountered.

     Refer to Attachment 3 in the **Information Access Management Policy** for a copy of the ***End User Security Policy Agreement.***

CITATIONS

45 C.F.R § 164.312(a)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XVII – AUDIT CONTROLS

IMPLEMENTATION SPECIFICATIONS

This standard is REQUIRED by 45 C.F.R. § 164.312(b)

POLICY

HIE shall ensure that access to information systems is properly controlled and restricted to authorized individuals. Certain systems have the capability to produce audit trails (i.e., audit control mechanisms) to record and examine system, network, and/or application activity. Periodically, the Security Officer shall review audit trails to detect and research security breaches (including high-risk patterns), to confirm/deny Users' compliance with HIE policies and procedures, and to identify potential weaknesses.

PROCEDURE

Auditing procedures are identified in the **Review** section of the **Security Management Policy**. Data included in audit trails shall include, without limitation, User ID, data source, provider, details of information, time of the access, and other relevant User information. If suspect activities or non-compliance is identified, disciplinary actions shall be enforced and documented, as discussed in the **Sanction** section of the **Security Management Policy**. If control weaknesses are identified, the Security Officer shall work to strengthen system controls to prevent reoccurrence.

CITATIONS

45 C.F.R § 164.312(b)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XVIII – INTEGRITY CONTROLS

IMPLEMENTATION SPECIFICATIONS

The following implementation specification is ADDRESSABLE pursuant to 45 C.F.R. 164.312(c)(1):

- **Mechanism to Authenticate Electronic Protected Health Information**

POLICY

HIE shall ensure that EPHI has not been changed/corrupted and to validate that data came from the original sender. Certain systems that process EPHI shall utilize controls to ensure the accuracy and Integrity of data at rest as well as in the processing cycle.

PROCEDURE

(a) Standards for data integrity – HIE shall use up-to-date industry- and system-appropriate mechanisms to authenticate EPHI. HIE shall maintain data Integrity in accordance with NIST standards. HIE shall implement electronic mechanisms to corroborate that EPHI has not been altered, destroyed, or intercepted in an unauthorized manner. HIE shall stay abreast of developments in the field of cryptographic message authentication and other fields related to verifying data integrity and authenticity.

(b) Technical components of data integrity – All data shall be accessed using, at a minimum, a user ID and password. HIE shall consider incorporating additional controls, for example, security questions and physical tokens where appropriate. HIE shall use allowed character checks, cardinality checks, consistency checks, cross-system consistency checks, data type checks, file existence checks, format and picture checks, batch and hash totals, logic checks, presence checks, limit and range checks, etc. on all incoming data. HIEs may incorporate check digits into unique identifiers. HIE shall use Poly1305-AES, UMAC, VMAC, or a message authentication code system that the Security Officer reasonably determines better serves the purpose of the HIE, to verify the integrity and authenticity of all messages. HIE shall monitor changes in technology and develop plans to transition quickly from unsecure systems. HIE shall consider implementing simultaneous redundant security, authentication, and integrity programs to protect EPHI in the event that it becomes compromised.

(c) Record of review – HIE shall store all transactions (rejected and accepted), log all changes/exceptions, and produce error reports. HIE shall implement controls to provide virus protection, continue processing during downtime, and provide error recovery.

CITATIONS

45 C.F.R § 164.312(c)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XIX – AUTHENTICATION CONTROLS

IMPLEMENTATION SPECIFICATIONS

This standard is REQUIRED by 45 C.F.R. §164.312(d)

POLICY

HIE shall ensure that access to information systems is properly controlled and restricted to authorized individuals. Authorization controls refer to the type of access that allow a User into HIE's systems. Such controls shall be restricted by role/function and/or individual User. HIE shall implement authentication controls that: (i) verify that the User is authorized and the one claimed; and (ii) deny access to unauthorized Users, programs, and/or processes. HIE has implemented procedures for ensuring that external users are properly authenticated to HIE's systems/network.

PROCEDURE

[Include details of managing authentication controls]

1. **Authorization Controls** – Users requiring access to EPHI shall obtain prior approval from assigned personnel. Additionally, Users shall sign the ***End User Security Policy Agreement*** indicating responsibility/accountability for appropriate consent and disclosure to authorized personnel only. Access, whether role- or user-based, shall be provided based on minimum necessary requirements for performing daily job activities. (See **Information Access Management Policy**)

2. **Entity Authentication** – HIE Users requiring access to HIE's systems/network shall first be approved for access, sign a ***Systems Access Request/Renewal Form***, and be granted a unique User ID and Password or personal identification number (PIN), depending on the system, based on function/role (i.e., minimum necessary information required). Additionally, every system HIE User shall log off upon completion of system use. Controls shall be implemented on some systems to automatically log off HIE Users after a period of inactivity to help prevent false identification and/or liability of a particular HIE User in the event of a security breach. Remote system access to HIE's systems for access of EPHI shall require **[name authentication method such as a token, secure ID card, unique ID/Password, PIN, digital signature, etc.]**.

CITATIONS

45 C.F.R § 164.312(d)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

ARTICLE XX – TRANSMISSION SECURITY

IMPLEMENTATION SPECIFICATIONS

The following implementation specifications are ADDRESSABLE pursuant to 45 C.F.R. §164.312(e)(1):

- **Integrity Controls**
- **Encryption**

POLICY

HIE shall take certain measures when EPHI is sent outside of HIE (e.g., via company network, e-mail, etc.) as well as establish the appropriate use of encryption to protect stored EPHI. Whenever EPHI is transmitted over an open network such as the Internet, technical controls, including Integrity controls and encryption, shall be implemented.

1. **Integrity** – When EPHI is transmitted outside of HIE or into HIE from another party, Integrity controls shall be implemented to ensure that data accuracy is maintained.

2. **Encryption** – HIE shall use encryption whenever EPHI is sent outside of HIE. In addition, encryption may be appropriate for other types of information including, but not limited to, e-mail containing other sensitive information and electronic files containing User credentials (e.g. usernames and Passwords) for systems that contain EPHI.

PROCEDURE

[Include the types of data to which transmission security shall apply]

1. **Electronic Protected Health Information (EPHI)** – Any type of information or data containing any one of the patient identification data elements (as defined by HIPAA) shall be sent outside of HIE only when it is encrypted.

   All department managers shall identify uses for, and employees who require, encryption and shall ascertain that appropriate equipment, training, and software are available so that necessary material is encrypted.

2. **Electronic Mail** – E-mail shall be considered the electronic equivalent of a post card. There shall be no assumption of Confidentiality when using e-mail over public networks. Unless the material is encrypted, Users shall not send EPHI or other sensitive HIE information over public networks or via e-mail.

3. **Password Encryption** – Passwords shall always be encrypted when held in storage or when transmitted over networks. Applications and operating systems shall not store User Passwords in clear text.

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.

4. **Use Approved Encryption Only** – Prior to use, encryption processes shall first be approved through the information technology department and/or the Security Officer.

CITATIONS

45 C.F.R § 164.312(e)

These Model Policies shall serve as GUIDANCE ONLY and can be modified, to the extent allowed by law, based on the HIE's size, technology and resources. These policies shall not be used as a standard by which to measure compliance with state or federal medical privacy law.