TEXAS HEALTH SERVICES AUTHORITY
HEALTH INFORMATION MODEL POLICY
REGARDING PRIVACY 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

PAGE

THSA Model Privacy Policies & Procedures

Update & Modification Timeline

Version	Date	Article	Page	Description of Modification
1.0	11/07/2012	All	All	Initial draft released.
1.1	05/28/2013	All	All	Policies updated to reflect passage of HITECH final omnibus rule.
1.2	08/20/2013	XI	32-34	Updated Policies to reflect passage of Texas Senate Bill 1609.
1.2	08/20/2013	XVIII	59	Updated Policies to reflect passage of Texas Senate Bill 1610.
1.3	09/30/2013	XVII	52	Corrected breach notification timelines to comply with only HIPAA/HITECH requirements, and not DURSA breach requirements.

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 Privacy Policies; the Model Security Policies are contained in an accompanying document.

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 has 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 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, which cover approximately 90% of the state's physicians and hospitals eligible for the program. The purpose of these Model Privacy Policies 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.

THSA Model Privacy Policies. These Model Privacy Policies are not intended to be exhaustive or one-size-fits-all, and Local HIEs are not required to adopt the policies verbatim; rather, the Model Privacy 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 PHI.

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 PHI by Local HIEs throughout the state varies considerably. Thus, while the policies herein 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 PHI, and the Model Policy was developed to comply with applicable law and to implement best practices. Thus, Local HIEs may choose to adopt this policy in its entirety, or to use this policy as a resource to

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

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.

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 in Texas 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."
>
> 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 of 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 PHI 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 PHI.

[2] *See* 45 C.F.R. §§ 160.103.

A model Business Associate Agreement is attached hereto as Appendix A (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, etc., HIEs should also require such subcontractors to execute Business Associate Agreement, which is intended to further ensure the privacy and security of patient PHI. 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.

Note: These definitions and other provisions in the Model Policies may change as the law in this area continues to evolve.

ARTICLE II - DEFINITIONS

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

Breach Notification Rule - the requirements set forth in Subpart D of 45 C.F.R. Part 164.

Business Associate - 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 PHI 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 PHI. In the HIPAA Omnibus Rule, the OCR specified that an HIE is a Business Associate.

Business Associate Agreement - 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 on behalf of the Covered Entity.

Centralized HIE - means a centralized architecture model 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.

Covered Entity - 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. (See page 6 for the definition of "Texas Covered Entity")

Data Use Agreement - written agreement which is required before a Covered Entity may use or disclose a limited data set (other than in situations where a limited data set is being used to satisfy the minimum necessary standard) so that a Covered Entity may obtain satisfactory assurance that the limited data set recipient will only use or disclose the PHI for limited purposes. A Data Use Agreement must (i) establish the permitted uses and disclosures of the information and may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the Privacy Standards or Security Standards if done by the Covered Entity; (ii) establish who is permitted to use or receive the limited data set; and (iii) provide that the limited data set recipient will (a) not use or further disclose the information other than as permitted by the data use

agreement or as otherwise required by law; (b) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement; (c) report to the Covered Entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware; (d) ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and (e) not identify the information or contact the individuals. There is no prescribed form for a Data Use Agreement, which may be a formal contract, an informal memorandum of understanding or, if the use of the limited data set is by a Covered Entity's workforce members, the Covered Entity may choose to enter into a data use agreement with those workforce members similar to the manner in which a Covered Entity would enter into a confidentiality agreement with its workforce members.

Designated Record Set – A designated record set includes:

A. Records and billing records about individuals maintained by or for a covered health care provider; or

B. A group of records used, in whole or in part, by or for the covered entity to make decisions about individuals; or

C. The enrollment, payment, claims adjudications, and case or medical management record systems maintained by or for a health plan.

The term "record" (as used in the context of a "designated record set") means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

The term "billing record" (as used in the context of a "designated record set") means a record that describes charges for services provided to a patient by a covered entity.

Effective Date - [Insert effective date here]

Federated HIE - An HIE architecture model 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.

HHS - United States Department of Health and Human Services.

HIE - The electronic movement of health-related information among organizations according to nationally-recognized standards.

HIETexas - A network of connections between participants in Texas that operates for the purpose of facilitating the private and secure sharing of health data in accordance with Applicable law.

HIPAA - Health Insurance Portability and Accountability Act as codified in 45 C.F.R. 160, 162, 164, and any and all amendments, including any and all amendments under HITECH, as adopted under the HIPAA final omnibus rule.

HITECH Act - Health Information Technology for Economic and Clinical Health Act, Division A, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), 42 U.S.C. 83000 *et seq.*, and implementation, regulations, and guidance.

Hybrid HIE – An HIE architecture model that incorporates aspects of both a federated and a centralized architecture model

IIHI - shall mean individually identifiable health information and shall have the meaning set forth in 45 C.F.R. § 160.103.

Individual – The person ("patient") who is the subject of the protected health information at issue and shall have the meaning set forth in 45 C.F.R. § 160.103, and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

Patient Participant – A patient who accesses, receives, or transmits PHI to or from a Local HIE who is not defined as a "Participant" below. (NOTE: inclusion of this definition depends on whether the HIE offers a patient portal by which individuals may access the HIE directly, and are not required to access the HIE through a participant.)

IRB– Means an "Institutional Review Board" established in accord and for the purposes expressed in 45 C.F.R. Part 46.

Local HIE -- one of the 12 regional HIE networks which cover approximately 90% of the state's physicians and hospitals eligible to participate in the statewide health information exchange.

Model Privacy Policies - Texas Health Services Authority Health Information Model Policy Regarding Privacy of Health Information, including all Articles and Appendices.

ONC - Office of the National Coordinator for Health Information Technology.

Participant - an individual or entity that accesses, receives or transmits PHI to or from the Local HIE, and enters into a Participation Agreement with HIE.

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

PHI – shall mean protected health information and shall have the meaning set forth in 45 C.F.R. § 160.103.

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

Required by Law - compelled by a mandate contained in a law that is enforceable in a court of law.

Secretary - the Secretary of the United States Department of Health and Human Services.

Security Standards - the Security Standards for the Protection of Electronic Protected Health Information set forth in 45 C.F.R. Parts 160 and 164.

Subcontractor – A person 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. A subcontractor is also considered a business associate where that function, activity, or service involves the creation, receipt, maintenance, or transmission of protected health information.

Texas Covered Entity - any person who: (i) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing. or transmitting PHI, including a Business Associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site; (ii) comes into possession of PHI; (iii) obtains or stores PHI under Chapter 181 of the Texas Health and Safety Code; or (iv) is an employee, agent, or contractor of a person described by (i), (ii), or (iii) of this definition insofar as the employee, agent or contractor creates, receives, obtains, maintains, uses, or transmits PHI.

THSA - Texas Health Services Authority created by Chapter 182 of the Texas Health and Safety Code.

TPO - treatment, payment, and healthcare operations.

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 Privacy 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 Privacy 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 PHI.

ARTICLE III - PRIVACY OFFICER

NOTE: While not a HIPAA or state law requirement, many HIEs may want to appoint a Privacy Officer. Some examples of responsibilities that the Privacy Officer could be assigned are listed below. Note that under HIPAA, HIEs are Business Associates and therefore are required to appoint a Security Officer. The Privacy and Security Officer may be the same individual. A sample Security Officer policy is included in the Model Security Policies section of this Model Policy.

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

POLICY

HIE may appoint a Privacy Officer to assume responsibility for developing, implementing, maintaining, and/or monitoring adherence to its privacy policies and procedures and/or the Privacy Standards or Security Standards. HIE should regularly update and maintain its documentation of privacy personnel designations, where applicable.

PROCEDURE

1. Privacy Officer. HIE may appoint a Privacy Officer to (i) report directly to its **[Chief Executive Officer, Senior Executive, and/or Health Information Management (HIM) Department Head]** and (ii) work with its **[Chief Compliance Officer, Chief Operating Officer, and/or General Counsel]** to ensure compliance with the Privacy Standards or Security Standards.

2. Qualifications. HIE may maintain certain qualifications of its Privacy Officer. The following is a non-exhaustive list of potential Privacy Officer qualifications that HIE may elect to require, either in whole or in part:

    a. education and experience relative to the size and scope of the respective organization;

    b. knowledge of (and experience with) information privacy laws, as well as accessing and releasing information and release control technologies;

    c. understanding of the Administrative Simplification provisions of HIPAA;

    d. knowledge in and the ability to apply the principles of health information management, project management, and change management;

    e. demonstrated organization, facilitation, communication, and presentation skills; and

f. current knowledge of applicable federal and state privacy laws and accreditation standards, and the ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.

3. Job Description. HIE may require its Privacy Officer to perform one or more of the following non-exhaustive list of duties, either in whole or in part:

a. Work with HIE's senior management and corporate compliance officer to establish an organization-wide interdisciplinary HIPAA task force to provide input on the development, implementation, and on-going review of privacy policies and procedures, as well as, assistance with implementation of these policies and procedures within each member's department.

b. Serve in a leadership role on the HIPAA task force referenced in Paragraph 3(a).

c. Designate a Contact Person **[which may be the Privacy Officer, a patient representative, one of Participant's administrative personnel, or an office]** (i) able to provide information about matters covered by the Notice of Privacy Practices, and responsible for receiving, responding to, and documenting complaints from employees, Business Associates, and others regarding their respective organization's privacy practices; (ii) responsible for conducting a thorough and timely investigation of all complaints lodged against their respective organization and assessing the viability and severity of the complaint; and (iii) responsible for coordinating correction, mitigation, and disciplinary action with the Privacy Officer, human resources department, and/or other appropriate persons and offices.

d. Regularly update and maintain documentation of privacy personnel designations and duties, including those for the Privacy Officer, the Contact Person (or office), and members of the HIPAA task force, including documentation regarding the hiring of a Privacy Officer and/or documentation showing that certain privacy duties have been added to the duties already handled by an existing employee and that those duties shall be maintained.

e. Perform a **[yearly, bi-annual]** privacy risk assessment of policies, procedures, and supervisory personnel responsible for privacy and security oversight, training programs, etc.; analyze whether there are any gaps; and determine timeframes and resources necessary to address any such gaps.

f. Work with appropriate legal counsel, management, key departments, and committees to ensure HIE and/or its Participant has, and maintains, sufficient privacy and confidentiality consent and authorization forms, as well as, information notices and materials reflecting current organizational and legal practices and requirements.

g. Identify, implement, and maintain HIE's privacy policies and procedures in coordination with management and administration, the HIPAA task force, and legal counsel.

h. Ensure that the privacy policies and procedures are regularly reviewed and updated.

i. Prepare a report on a periodic basis for **[the Board, CEO, corporate officers, and HIPAA task force]** regarding both the status of implementing and maintaining the privacy program and future requirements to implement and maintain compliance.

j. Oversee delivery of initial privacy training on privacy policies and procedures to all employees, volunteers, medical and professional staff, board members, and other appropriate parties.

k. Document (and maintain documentation) that all required training has occurred in a timely manner.

l. Initiate, facilitate, and promote activities to foster information privacy awareness within HIE (and its related entities).

m. Ensure that all members of HIE's workforce are informed when policies and procedures are changed or updated.

n. Evaluate adherence to HIE's privacy policies and procedures by all departments and personnel.

o. Conduct ongoing compliance monitoring activities in coordination with HIE's other compliance and operational assessment functions.

p. Initiate and conduct an internal privacy audit program.

q. Establish, with HIE's management, operations, and Security Officer, a mechanism to track access to PHI within the HIE's purview (and as also may be required by law), and allow qualified individuals to review or receive a report on such activity.

r. Work cooperatively with other applicable HIE units, including Business Associates and Participants, in overseeing patient rights to inspect and amend PHI as appropriate, and restrict access to PHI when appropriate.

s. Work with HIE's **[Security Officer, Contact Person (or office), Corporate Compliance Officer, director of human resources, and/or legal counsel]** to establish a process for receiving, documenting, tracking, investigating, and taking corrective action on all complaints concerning the HIE's privacy policies and procedures (including self-disclosures).

t. Develop appropriate sanctions for failure to comply with privacy policies and procedures.

u. Implement consistent application of sanctions to all individuals in HIE's workforce, extended workforce, and for all Business Associates, in cooperation with **[the Security Officer, human resources department, administration, and/or legal counsel]**.

v. Implement corrective action to mitigate effects of inappropriate use or disclosure of PHI and document such actions.

w. In collaboration with legal counsel, identify Business Associates that receive PHI and review existing contracts with these entities for compliance with HIPAA.

x. Review and evaluate proposed business contracts and other documents to identify and correct potential conflicts between HIE's privacy policies and procedures and applicable federal and state laws and regulations.

y. Cooperate with HHS, OCR, other legal entities, as well as, HIE officers, in any and all compliance reviews or investigations.

z. Set and track potential performance measures, which may include:

   i. the number of breach of confidentiality/privacy infringement-related complaints;

   ii. the number of claims/suits alleging confidentiality/privacy breaches;

   iii. regulatory fines related to confidentiality/privacy issues;

   iv. the number of internal incidents involving violations of privacy policies;

   v. percentage of HIE's workforce members receiving privacy training on time and according to mandated schedules;

   vi. percentage of HIE's workforce with current confidentiality/privacy certifications on file; and

   vii. accrediting agency citations involving confidentiality/privacy.

aa. Serve as a member of, or liaison to, HIE's IRB and/or Privacy Board (to the extent applicable).

bb. Serve as the information privacy liaison for users of clinical and administrative systems.

cc. Review all system-related information security plans throughout HIE's network to ensure alignment between security and privacy practices, and act as a liaison to the information systems department and the Security Officer.

REFERENCES/CITATIONS

Privacy officer: 45 C.F.R. § 164.530(a)(1)(i)

65 Fed. Reg. 82462, 82561, 82744-45, 82767-68, 82782-83 (Dec. 28, 2000)

Contact Person: 45 C.F.R. §§ 164.520(b)(1)(vii), 164.524(d)(2)(iii), 164.526(d)(1)(iv), 164.530(a)(1)(ii) (2013)

65 Fed. Reg. 82462, 82548, 82550, 82557, 82561-62, 82747 (Dec. 28, 2000); 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

ARTICLE IV - CONSENT OR AUTHORIZATION

POLICY

In this policy, use of the terms "consent" or "authorization" or the phrase "consent or authorization" refers to the patient permission that is required, and includes all required elements, for uses and disclosures of the patient's PHI under state and federal law.

Unless specifically excepted or permitted under HIPAA or Texas privacy law, a patient's PHI may not be used or disclosed without a valid consent or authorization from the patient.

Under HIPAA, a patient authorization is not needed if PHI is used or disclosed as permitted by the HIPAA Privacy Rule. For all other purposes, a patient authorization will be required. However, it is important to note that federal and state laws also provide privacy protections for certain classes of PHI above and beyond the protections generally provided by HIPAA. The following classes of information are among those requiring special consideration: (i) substance abuse records, (ii) psychotherapy notes, (iii) AIDS test results, (iv) genetic information, (v) mental health records, (vi) mental retardation records, (vii) mental health research results, and (viii) controlled substance research results. State laws also prohibit many health care providers and others with access to patient health care information from disclosing that information without consent or authorization, subject to certain exceptions, which may or may not be as broad as the exceptions contained under HIPAA for treatment, payment and health care operations. Additionally, federal law specifies that Business Associates, such as HIEs, may only use or disclose PHI as allowed under its Business Associate Agreement with the relevant Covered Entity except Business Associates must disclose PHI when required by the Secretary and as needed to comply with the Covered Entity's obligations regarding patients' requests for an electronic copy of their own records. Any limitations in the Business Associate Agreement between the HIE and the Covered Entity must be passed down in the related Business Associate Agreement should the HIE engage a subcontractor.

Under the Texas Medical Records Privacy Act, HIE and its Participants are prohibited from electronically disclosing PHI to any person without a separate authorization from the individual or his or her legally authorized representative for each disclosure, unless the disclosure is made: (i) as otherwise authorized or Required by Law, or (ii) to another Texas Covered Entity or a "covered entity" as that term is defined by Section 602.001 of the Texas Insurance Code, for the purpose of treatment, payment, health care operations, or performing an insurance or health maintenance organization function described by Section 602.053 of the Texas Insurance Code. The authorization may be given in writing, either in hard copy or electronic form, or orally if it is documented in writing by HIE or its Participant. The Act further provides that the attorney general of Texas will adopt a standard authorization form for use in complying with the law. This authorization shall be written in plain language and made available in languages other than English in conformity with Title VI of the Civil Rights Act of 1964.

HIE is not required by law to obtain separate or additional consent or authorization from a patient if the Participant has already obtained such patient's consent or authorization. In general, if the Participant has the right to disclose the information, and HIE is working on behalf of the

Participant pursuant to a BAA and Participation Agreement to disclose the information, then the HIE would not need to obtain any additional consent or authorization from the patient for the disclosure of the patient's PHI.

However, many HIEs do elect, in collaboration with their Participants, to employ a patient consent or authorization model that is above the specific consent or authorization requirements that are already Required by Law. For example, some Participants may require consent or authorization for uses and disclosures of PHI for treatment, payment and health care operations when not Required by Law. Other Participants and HIEs may employ an "opt-in" or "opt-out" model as set forth in Article V below to determine a patient's preference, for the transmission of PHI to or by an HIE as an example.

HIEs should work with their Participants and legal counsel of their HIE and Participants to carefully identify what types of information will be used or disclosed by the HIE, what consents or authorizations may be required for such uses and disclosures and which party will be responsible for obtaining and maintaining such consents or authorizations. Local HIEs may want to include in their BAA and Participation Agreements a warranty or representation that the Participant has obtained all necessary consents or authorizations regarding the use or disclosure of these classes of records. Likewise, Local HIEs may want to consult an attorney, or encourage their Participants to consult legal counsel, prior to releasing these categories of information in order to ensure the proper patient consent or authorization has been obtained.

REFERENCES/CITATIONS

45 C.F.R. §§ 164.502-164.508. (2013)

65 Fed. Reg. 82462, 82513-21, 82650-62 (Dec. 28, 2000); 67 Fed. Reg. 53182, 53219-53226 (Aug. 14, 2002)

78 Fed. Reg. 5599-5602 (Jan. 25, 2013)

Civil Rights Act of 1964, 42 U.S.C. § 2000d *et seq.*; 45 C.F.R. § 80.3(b)(2) (2001); 65 Fed. Reg. 52762 (2000) (Policy Guidance on the Prohibition Against National Origin Discrimination as it Affects Persons with Limited English Proficiency)

TEX. HEALTH & SAFETY CODE § 181.154, as added by HB 300.

ARTICLE V - PATIENT PREFERENCE

POLICY

HIEs may elect to determine a patient's preference as to uses, disclosures, or transmission of that patient's PHI even if not Required by Law. For example, although not required by HIPAA, an HIE may elect to employ an opt-in or opt-out model to determine a patient's preference as to the transmission of PHI to or by HIE, or to give the patient the opportunity to object to such transmission.

PROCEDURE

Should HIE elect to obtain a patient's preference through an opt-in or opt-out model, HIE may choose to directly manage the process of obtaining patient preference or request a Participant to do so through its agreement with such Participant. The process for a patient to opt-in or opt-out should be fair and not burdensome.

1. Patient Preference Form. Depending on how the HIE is structured and its process for obtaining any such elections, patients may be asked to read and sign a patient preference form and/or HIE may also provide notice on its website that individuals have the right to opt-in or opt-out. HIE will provide additional guidance on the Patient Preference Form reminding the individual that "opting-out" removes the individual's health information from only that Local HIE, and that the individual's health information may still reside in other Local HIEs. It is important to note that using an opt-in or opt-out model will not obviate the need for obtaining a consent or authorization for certain uses or disclosures that includes all elements, or information, Required by Law.

2. Who May Express Preference. In general, it is the individual that is the subject of the PHI, or his or her personal representative, who is given the right to express a preference as to the exchange of his or her PHI by HIE. Additionally, the individual may also designate someone -- a family member, caregiver, domestic partner or legal guardian -- to make the decision on his or her behalf.

3. When Patient Preference Must be Obtained. An HIE that has a patient preference policy should consistently and fairly implement that policy. To the extent that an HIE has made representations about its patient preference policy, the HIE should carefully consider how changing that policy or failing to abide by it could result in legal liability for the HIE.

4. The Information Exchanged. HIE may want to consider offering choices or technical solutions to individuals that allow them to indicate their preference as to the use of certain information being transmitted to or exchanged by HIE rather than having to determine whether to allow either all or none of their PHI to be transmitted to or exchanged by HIE. [NOTE: Local HIE should collaborate with its Participants and other stakeholders to determine the proper level of implementation of this policy before offering the choices discussed herein.]

ARTICLE VI - NOTICE OF DATA PRACTICES, ELECTRONIC DISCLOSURE

POLICY

While HIE's primary purpose is to facilitate the transmission of health data, in order to comply with State Law, HIE shall provide written notice to patients for whom it creates or receives PHI if the PHI is subject to electronic disclosure. The written notice should be on the HIE website. HIE employees who maintain the HIE's website shall be familiar with this Policy and shall follow these procedures. HIPAA Covered Entities are required to provide to their patients and maintain a Notice of Privacy Practices. The HIE as a Business Associate is not required to maintain a HIPAA Notice of Privacy Practices, but may work with Participants to include language in their HIPAA Notice of Privacy Practices regarding transfer or exchange of PHI to or by an HIE.

PROCEDURE

Post Written Notice of Possible Electronic Disclosure of PHI. HIE shall provide general notice to patients that their PHI is subject to electronic disclosure by posting a written notice on HIE's Internet website.

Provide Language to Include in Participants' Notice of Privacy Practices. HIE and Participant may deem it beneficial for HIE to develop language that can or must be included in Participants' Notices of Privacy Practices regarding transfer or exchange of PHI to or by HIE. To the extent that such privacy practices may change over time, HIE and Participant may want to ensure that Participant retains the right, as part of any such language, to change its privacy practices at any time by updating the notice.

REFERENCES/CITATIONS

TEX. HEALTH & SAFETY CODE § 181.154, as added by H.B. 300.

ARTICLE VII - ACCOUNTING OF WHO HAS ACCESSED PHI AND TO WHOM PHI HAS BEEN DISCLOSED

[COMMENT: THIS SECTION DOES NOT INCORPORATE CONCEPTS FROM PROPOSED RULE ON ACCOUNTING OF DISCLOSURES ISSUED IN MAY 2011 THAT INTRODUCED CONCEPT OF ACCESS REPORTS. IN THE PROPOSED RULE, OCR PROPOSES REVISING THE PRIVACY RULE TO CREATE TWO SEPARATE RIGHTS FOR INDIVIDUALS: THE RIGHT TO AN ACCOUNTING OF DISCLOSURES AND THE RIGHT TO A REPORT ON ACCESS.]

POLICY

HIE recognizes an individual's right to receive an accounting ("accounting") of certain disclosures of an access to the individual's PHI made by HIE in the six years prior to the date on which the accounting is requested. HIE employees whose responsibilities include receiving requests for accountings and processing and providing accountings shall be familiar with this Policy and shall follow these procedures. HIE shall consult its BAA and Participation Agreement with a Participant to determine any specific timing or other requirements.

PROCEDURE

1. Designation of Person or Office Responsible for Accountings. HIE hereby designates **[Contact Person]** as the person or office responsible for receiving and processing requests for an accounting.

2. Recognize an Individual's Right to Request an Accounting. HIE shall recognize an individual's right to receive an accounting of certain disclosures of the individual's PHI made by HIE and/or of who has access the individual's PHI through HIE in the six years prior to the date on which the accounting is requested. If HIE receives a request for an accounting from an individual relating to such individual's PHI, HIE shall promptly forward such request to the applicable Participant, which shall follow its own Policies with respect to requests for accounting.

3. Determine the Time Period of the Request. An individual who requests an accounting shall complete a written request that includes the time period within which the disclosures requested must have occurred. An individual may request an accounting for any period of less than six years from the date of the request.

4. Acting on an Individual's Request for an Accounting.

    a. Create the Accounting of Disclosures. HIE shall act on each individual's request for an accounting within the time periods set forth in paragraph 5 of this Policy, and shall include all required disclosures and other information in accordance with paragraphs 4(b) and (c) of this Policy. The term "disclosures" includes disclosures of an individual's PHI made by HIE's subcontractors unless the disclosure is excepted from the accounting requirements. If an individual requests an accounting, HIE will contact its subcontractors to whom HIE has disclosed the

individual's PHI and obtain an accounting of disclosures that are subject to an accounting made by the subcontractors with respect to the individual's PHI.

b. Exceptions From Disclosure. As requested, the accounting shall include a description of who has accessed, and any disclosures of, the individual's PHI made by HIE in the time period chosen by the individual. However, the accounting is not required to include any of the following disclosures:

i. to carry out treatment, payment and health care operations

ii. to individuals regarding their own PHI;

iii. for national security or intelligence purposes;

iv. to correctional institutions or law enforcement officials;

v. authorized by the individual according to Article IV (Authorization) of these Model Privacy Policies;

vi. incidental to a permitted use or disclosure; or

vii. as part of a limited data set pursuant to a Data Use Agreement.

c. Include Other Required Information in the Accounting. The accounting shall further include, for each access and/or disclosure:

i. the date of the access or disclosure;

ii. the person accessing or recipient of the PHI and the address, if known;

iii. a description of the information accessed and/or disclosed; and

iv. a statement of the purpose of the access and/or disclosure or a copy of the individual's written request for access or a disclosure.

d. Process for Accounting for Multiple Instances of Access or Disclosures. If, during the period covered by the accounting, HIE has made multiple disclosures of PHI, or provided access to PHI on more than one occasion, to the same person or entity for a single purpose as requested by the individual, the accounting may, with respect to such multiple disclosures, provide:

i. the information required by paragraph 4(c) of this Policy for the first access or disclosure during the accounting period;

ii. the frequency, periodicity, or number of the instances of access or disclosures made during the accounting period; and

iii. the date of the last such access or disclosure during the accounting period.

5. Time Period for Acting on an Individual's Request for an Accounting. Subject to the terms of its BAA and/or Participation Agreement, HIE may provide the accounting to the Participant to forward to the individual or provide the accounting directly to the individual. HIE shall consult its BAA and Participation Agreement with a Participant to determine the appropriate time frame but shall act on each individual's request for an accounting no later than 60 days after receipt of such a request, as required by law, as follows:

    a. Provide the accounting requested; or

    b. Obtain an extension for no more than 30 additional days and provide a written statement of the reasons for the delay.

6. Fees. The first accounting to an individual in any 12-month period shall be without charge. A reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period will be charged. HIE shall inform the individual in advance of the fee and provide the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

7. Required Documentation. HIE will document the following and retain the documentation for six years from the date when the information was created or was last in effect:

    a. The written accounting that is provided to the individual in accordance with this Policy;

    b. The information required to be included in an accounting as set forth in paragraphs 4 and 5 of this Policy; and

    c. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

REFERENCES/CITATIONS

HITECH § 13405(c)

45 C.F.R. § 164.528 (2013)

65 Fed. Reg. 82462, 82506, 82559-61, 82672, 82692, 82739-44, 82784 (Dec. 28, 2000); 67 Fed. Reg. 53182, 53243-47, 53271-72 (Aug. 14, 2002)

ARTICLE VIII - ACCESS TO INSPECT AND COPY RECORDS

POLICY

HIE shall recognize an individual's right to access (*i.e.*, inspect and/or obtain copies) of his or her own PHI contained in a designated record set, if it is determined that the individual is entitled to access. While HIE may or may not maintain PHI in a "designated record set," as defined by HIPAA, HIE must comply with this policy to the extent possible in HIE's capacity as a HIPAA business associate. In the case of a request from an individual, the BAA and/or Participation Agreement will normally dictate whether the HIE provides this information to an individual or forwards the request to the Participant, which shall manage the process. HIE employees who receive patient requests to inspect and copy records shall be familiar with this policy and shall follow these procedures.

Editor's Note: Based on the HIE's model, HIE may or may not maintain PHI in a designated record set. This article addresses one or more issues regarding HIEs that do maintain PHI in a designated record set. For those HIEs that do not maintain PHI in a designated record set, this article may be modified according to the model utilized by that HIE.

PROCEDURE

1. Access Only to Information in a "Designated Record Set." If Participant asks HIE to provide access to information, HIE is required to provide access only to information contained in the following designated record sets:

   a. Medical records;

   b. Billing records; and

   c. Other records containing information used, in whole or in part, to make decisions about the individual, whether or not the records have been used to make a decision about the individual.

   An individual shall have access to this information, from either HIE or Participant as described above, for as long as it is maintained in a designated record set. If the information requested is not part of a designated record set, the individual has no right of access to it. The Privacy Officer shall determine what PHI is in the individual's designated record set and is accessible to the individual.

2. Notification of Participant. If an individual submits a written request for an opportunity to inspect and/or obtain copies of his or her PHI to HIE, subject to the terms of the BAA and/or Participation Agreement, HIE shall promptly notify Participant of such request in

writing, in order to give Participant the opportunity to respond to such request. If Participant requests that HIE provide the requested information to the individual, HIE shall follow the procedures set forth in this Policy. In the alternative, Participant may elect to respond to the request, in which case it must notify HIE in writing of such response. If Participant elects to respond, HIE shall promptly notify the Individual the Participant will be responding to his or her request directly. **[If Participant does not notify HIE of its intent to respond to such request within _____ business days of its receipt of the request from HIE, [or if the individual notifies HIE that it has not received a response from Participant and ____ business days have elapsed since Participant notified HIE that it intended to respond,]** HIE should notify the individual that the Participant has not responded.] If HIE receives a written request from Participant to inspect and/or obtain copies of PHI related to Participants' operations, HIE shall follow the procedures set forth in this Policy. Any PHI provided by HIE, to either individuals or Participants, shall be in a readable form and format.

3. Providing Access to Records in the Designated Record Set. If (a) an individual makes a valid request for access to PHI and Participant requests that HIE make the disclosure, or (b) Participant makes a valid, written request for access to PHI, the following steps should be taken:

   a. Notify the individual and grant access (make the information available for examination or provide a copy) as promptly as required under the circumstances but not later than 15 days after receiving the request.

   b. HIE shall provide the individual or Participant with access to the information in the form or format requested if it is readily producible. If the form requested is not readily producible, the information may be produced in a readable hard copy format.

      i. If the individual or Participant is requesting personal access to inspect or copy, arrangements should be made to arrange a convenient time for inspection and copying of the records.

      ii. If an individual or Participant requests that PHI be mailed to him, her or it, HIE shall honor that request if fees for copying and mailing are paid in advance. If the requested PHI may be provided more quickly and inexpensively in an electronic format, the individual or Participant shall be notified of this option.

      iii. If an individual or Participant requests PHI that HIE maintains in an electronic health record, the individual or Participant shall have a right to obtain from HIE a copy of such information in the electronic form and format specified by the individual if it is readily producible in such format or in a readable electronic form agreed upon by the Provider and the individual if it is not, if the individual or Participant chooses, to direct HIE to transmit such copy directly to an entity or person designated by the

individual, provided that the request is in writing, signed by the individual, and clearly identifies the designated person to whom to send the PHI and the location at which to find the designated person.

iv. An individual or Participant may be provided with a summary of the requested PHI rather than specific information if:

(1) the individual or Participant agrees to receive a summary;

(2) the individual or Participant agrees in advance to any fees that will be imposed in preparing the summary; and

(3) a summary is permitted by and in accordance with state law.

v. If access to PHI is denied in part for the reasons stated in paragraph 5(a) of this Policy, HIE shall provide the individual or Participant with access to the PHI that the individual or Participant has the right of access to, and exclude (through redaction) the PHI for which HIE has a ground to deny access.

c. Before PHI is released, the identity of the person or entity requesting the information shall be verified.

4. Fee Charged for Disclosure. HIE may charge the requestor a reasonable fee for the disclosure of PHI whether the information is provided in paper or electronically.

5. Denial of Access to PHI.

a. *Reasons for Denial*. HIE shall rely on the Participant to determine whether access or disclosure to an individual shall be permitted, and HIE shall not make its own decision to deny access. The Participant may deny access to PHI if the information is:

i. not part of a designated record set;

ii. psychotherapy notes;

iii. compiled by HIE **[or Participant]** in anticipation of a civil, criminal, or administrative action or proceeding;

iv. a test report or result held by a clinical laboratory regulated under the Clinical Laboratory Improvement Amendments ("CLIA") or a research laboratory exempt from CLIA if the individual is not an authorized person.

v. compiled during the course of a research study, in which case access may be denied until the completion of research if the participant agreed to this denial of access when consenting to participate in the clinical trial and was

informed that the right to access PHI will be reinstated at the conclusion of the clinical trial (however, access is allowed in certain situations, such as when an individual has a severe adverse reaction and needs the information to make a proper treatment decision);

vi. received from another source other than a health care provider under a promise of confidentiality, and providing access would reveal the source of the information;

vii. subject to the Privacy Act (5 U.S.C. § 552a) if such denial is permitted under the Privacy Act; or

viii. records that are subject to a legal privilege, including but not limited to, attorney-client privilege and the peer review privilege.

b. *Notice of Denial*. If access to an individual is to be denied in part or in whole, Participant shall inform HIE and the individual **[(or ask HIE to inform the individual)]** in writing, within ___ business days of the date of the initial request, of the following:

i. the specific grounds for the denial; and

ii. the right to protest the denial to Participant (with contact information) and to the Secretary.

c. *Review of Denial*. An individual may obtain review of a denial of access as follows:

i. Participant will designate a person not directly involved in the decision to deny access to be the designated reviewing official ("official"), and will promptly refer a request to that official;

ii. The official will determine within a reasonable period of time, whether to deny access based upon the criteria listed in this Policy, which decision by the official will be final; and

iii. Participant will promptly notify the requestor in writing **[(or ask the HIE to provide notification)]** of the determination of the official, and if the official finds that the requestor should be given access to inspect and/or copy his the PHI, HIE will provide that access as described in paragraph 3 of this Policy.

6. Document Retention. HIE shall retain documentation of the designated record sets that are subject to access by individuals and Participants and the titles of persons or offices responsible for receiving or processing requests for access in paper or electronic form for at least 6 years from the date when such documents were last in effect. HIE may be

required to provide accounting of who has accessed PHI and to whom PHI has been disclosed, pursuant to Article VII of these Model Privacy Policies.

REFERENCES/CITATIONS

45 C.F.R. §§ 160.202, 164.501, 164.514(h), 164.524 (2013)

HITECH § 13405(e)

65 Fed. Reg. 82462, 82485, 82504, 82538, 82547, 82548, 82554-58, 82593, 82605-07, 82731-36, 82764 (Dec. 28, 2000); 67 Fed. Reg. 53182, 53191, 53249 (Aug. 14, 2002)

78 Fed. Reg. 5631 (Jan. 25, 2013)

OCR Guidance, 28, 30, 44, 49 (July 6, 2001)

Clinical Laboratory Improvement Amendments, 42 U.S.C. § 263a; 42 C.F.R. part 493 (2002)

Privacy Act, 5 U.S.C. § 552a

TEX. HEALTH & SAFETY CODE ANN. §§ 181.102, as added by H.B. 300.

REQUEST FOR AMENDMENT OF RECORDS POLICY
(ALTERNATE POLICY TO ARTICLE IX BELOW)

Editor's Note: Based on the HIE's model, this policy may better fit the HIE's needs in complying with state and federal medical privacy law than Article IX below.

POLICY

HIE shall recognize an individual's right to request the amendment of PHI about the individual when the individual believes that the PHI is incorrect or inaccurate. In the case of a request from an individual, the BAA and/or Participation Agreement will normally dictate the process for responding, which may or may not require the Participant to manage the process. HIE employees whose responsibilities include receiving requests for amendment of records shall be familiar with this policy and shall follow these procedures. (NOTE: this policy dictates that requests for amendments to PHI should be directed to the Participant. If HIE wishes to incorporate a policy wherein HIE directly amends PHI maintained by HIE, then this policy should be modified accordingly.)

PROCEDURE

1. Requests made to Participant. Individuals should make requests to amend PHI to the Participant. Requests to amend PHI must be in writing and must include a reason to support the requested amendment.

2. Requests made directly to HIE. If HIE receives a written request from an individual to amend PHI about the individual, within ___ business days of receipt by HIE, HIE shall forward such request to the Participant for review.

3. Maintenance Log. HIE shall maintain a log of all requests for amendments to PHI made directly to HIE.

ARTICLE IX - REQUEST FOR AMENDMENT OF RECORDS

POLICY

Subject to the review and approval of Participant, HIE shall recognize an individual's right to request the amendment of PHI about the individual in a designated record set for as long as the PHI is maintained in a designated record set when the individual believes that the PHI is incorrect or inaccurate. In the case of a request from an individual, the BAA and/or Participation Agreement will normally dictate the process for responding, which may require the Participant to manage the process. HIE employees whose responsibilities include receiving requests for amendment of records shall be familiar with this policy and shall follow these procedures.

Editor's Note: Based on the HIE's model, HIE may or may not maintain PHI in a designated record set. This article addresses one or more issues regarding HIEs that do maintain PHI in a designated record set. For those HIEs that do not maintain PHI in a designated record set, this article may be modified according to the model utilized by that HIE.

PROCEDURE

1. Processing a Request for Amendment. Requests for HIE to amend PHI must be in writing and must include a reason to support the requested amendment. If HIE receives a written request from an individual to amend PHI about the individual, within ___ business days of receipt by HIE, HIE shall forward such request to Participant for review. Participant shall make the determination, in its sole discretion, as to whether the PHI should be amended. HIE shall use its commercially reasonable efforts to obtain a decision in writing from Participant with respect to a requested amendment, including details with respect to the extent to which such amendment should be approved and any limitations and the basis for any denial, within **[60]** days.

2. Granting an Amendment.

    a. If Participant grants the request, HIE will:

        i. make the amendment to the PHI only to the extent specifically approved by Participant in writing by, at a minimum, identifying the records that are affected by the amendment and appending or otherwise providing a link to the location of the amendment;

        ii. inform the individual in writing, within ___ days of HIE's receipt of a decision from Participant, that the amendment has been accepted and obtain the individual's permission to notify the relevant persons with whom the amendment needs to be shared;

        iii. inform persons identified by the individual as needing notice of the amendment, or arrange for Participant to provide such notifications; and

iv. inform other such persons, such as subcontractors, that HIE knows to have/maintain the original PHI and who has relied or may foreseeably rely on the information to the detriment of the individual, or arrange for Participant to provide such notifications.

3. Denial of the Requested Amendment.

a. HIE will deny the amendment if it receives written notification from Participant that Participant has denied the amendment **[or is unable to receive a response with respect to the amendment from Participant within ___ days after providing notification of the request for amendment to Participant]**.

b. If HIE denies the amendment, based on the decision by Participant, it will provide the individual with a timely, written denial, which indicates:

i. the basis for the denial, as provided by Participant;

ii. that the individual has the right to submit a written statement of disagreement with HIE, which it will promptly forward to Participant, and that such a statement may be submitted to HIE by sending it to **[the Contact Person at _____]**;

iii. that if the individual chooses not to submit a statement of disagreement, the individual may instead request, in writing, that a copy of the request for amendment and HIE's denial, based on Participant's denial, be included with any future disclosures of the disputed PHI, which request HIE will promptly forward to Participant; and

iv. how the individual may complain to HIE, Participant or the Secretary, including the name, title, and telephone number of the Contact Person designated to receive these complaints on behalf of HIE.

c. [*Statement of Disagreement.* Individuals will be permitted to submit a written statement disagreeing with the denial of all or part of a requested amendment. The length of a statement of disagreement will be limited to [2 pages]. HIE will promptly forward any such statement to Participant.]

d. [*Rebuttal Statement.* HIE may request that Participant prepare a written rebuttal to the individual's statement of disagreement. If prepared, HIE will forward a copy of the written rebuttal to the individual promptly after HIE's receipt of such rebuttal from Participant.]

4. Record Keeping. HIE will identify the record or PHI that is the subject of any disputed amendment and will append or otherwise link the following information to the designated record set in which the PHI resides:

a. the individual's request for amendment;

b. HIE's denial of the request, based on Participant's denial;

c. the individual's statement of disagreement, if any; and

d. Participant's rebuttal, if any.

5. **[Future Disclosures. If a statement of disagreement has been submitted by the individual, HIE will provide the information in paragraph 4 of this Policy, or an accurate summary of this information, with any future disclosures of the PHI to which the disagreement relates. If the individual has not submitted a statement of disagreement, HIE will provide the information in paragraphs 4(a) and (b) of this Policy, or an accurate summary of this information, only if the individual has so requested.]**

6. Notices of Amendment From Other Entities. If HIE receives notice from another Covered Entity that an amendment to an individual's PHI has been made, HIE will notify Participant of such amendment and follow the procedures set forth in this Policy in making the determination as to whether to amend such PHI in its designated record sets.

7. Other Documentation. Documentation of the title of the person or office responsible for receiving and processing these requests on behalf of HIE will be retained for 6 years after it was last in effect.

8. Notifications to Participant. HIE will forward any notices, statements and other documentation related to proposed amendments to Participant promptly after receipt from the individual.

REFERENCES/CITATIONS

45 C.F.R. §§ 160.202 (definition of more stringent), 164.504(e)(2)(ii)(F), 164.504(f)(2)(ii)(F), 164.520(b)(1)(iv)(D), 164.526 (2001)

65 Fed. Reg. 82462, 82506, 82558-59, 82736-38, 82755, 82774, 82796 (Dec. 28, 2000); 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

ARTICLE X - REQUEST FOR RESTRICTIONS

POLICY

HIE shall recognize an individual's right to request the restriction of uses and disclosures of PHI and adhere to restrictions to which Participant has agreed, to the extent that Participant has provided HIE with written notice of such restrictions, in accordance with the Privacy Standards or Security Standards. Pursuant to the BAA or Participation Agreement, the Participant shall notify the HIE of any restrictions and require the HIE, as a Business Associate, to honor such restrictions. HIE employees who have the authority to disclose PHI shall be familiar with this Policy and shall follow these Procedures.

NOTE: Implementation of this article will be strongly dictated by the technology employed by HIE. Individual policies may need to be tailored to HIE's specific consent model (e.g., opt-in, opt-out, etc.).

Editor's Note: Please note that once the THSA's State-Level Shared Services are operational, Local HIEs will be subject to additional requirements that may be relevant to the procedures listed herein. Specifically, the THSA will require Local HIEs participating in State-Level Shared Services to notify the THSA of changes in patient consent preferences that will impact HIE-to-HIE communications.

PROCEDURE

1. Recognize an Individual's Right to Request Privacy Protection for PHI. Subject to the terms of its BAA and Participation Agreement with Participant, HIE shall adhere to any restrictions agreed to by Participant with limiting uses and disclosures of PHI about an individual to uses and disclosures necessary to carry out treatment, payment, or health care operations and disclosures to persons involved in the individual's care (collectively, "Restrictions"), if and to the extent that HIE has received written notice detailing the Restrictions from Participant. If HIE receives a request from an individual to agree to Restrictions with respect to PHI about the individual, within ___ business days of receipt by HIE, HIE shall forward such request to Participant to review. Participant shall make the determination, in its sole discretion, as to whether the PHI should be restricted. It is Participant's responsibility to notify the HIE and the individual of the Participant's determination. If Participant agrees to a Restriction, in addition to adhering to such Restriction, HIE shall notify its Business Associates of the Restriction, and the business associations will be required to adhere to the Restriction. If the individual requests privacy protection from a health plan with respect to an item or service for which the individual pays in full out of pocket and disclosure to the health plan would be for the purpose of payment or health care operations and such disclosure is not otherwise required by law, the HIE/Participant must grant the request and may not later terminate the Restriction.

2. Use and Disclose PHI in Accordance With Agreed Upon Restrictions. If Participant agrees to a requested Restriction, HIE may not disclose PHI in violation of the Restriction unless the individual who requested the Restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment; in such a case HIE may disclose PHI to a health care provider, to provide emergency treatment to the individual. If restricted PHI is disclosed to a health care provider for emergency treatment in accordance with this paragraph, HIE shall request the health care provider not to further use or disclose the information.

3. Do Not Prevent Certain Uses and Disclosures. A restriction agreed to by Participant and adhered to by HIE is not effective to prevent: (a) disclosures to the individual; (b) uses and disclosures that do not require individual permission; and (c) disclosures to the Secretary.

4. Terminating a Restriction. HIE may terminate its agreement to a restriction if:

   a. The individual agrees to or requests the termination in writing, in which case HIE shall promptly provide written notice of such agreement or request to Participant; or

   b. HIE receives written instruction from Participant to terminate the Restriction, **[in which case HIE shall promptly provide written notice to the individual that the HIE is terminating its agreement to a Restriction,] [except that such termination is only effective with respect to PHI created or received after HIE has informed the individual. HIE shall continue to comply with its former agreed-upon Restrictions with respect to PHI created or received prior to informing the individual of the termination]**.

   As stated above, Restrictions from a health plan for services paid for completely by the individual out of pocket may not be terminated except at the request of the individual.

5. Documentation of Agreed Upon Restrictions. If Participant agrees to a requested Restriction, HIE must document the Restriction in written or electronic form and shall maintain such documentation for 6 years from the date the Restriction was last in effect. A specific form of documentation is not required; a note in the medical record or similar notation is sufficient.

REFERENCES/CITATIONS

HITECH § 13405(a)

45 C.F.R. §§ 164.502(c), 164.522(a) (2013)

65 Fed. Reg. 82462, 82512, 82552-53, 82726-30 (Dec. 28, 2000); 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

78 Fed. Reg. 5626-30 (Jan. 25, 2013)

ARTICLE XI - ROLE-BASED WORKFORCE TRAINING

POLICY

All members of HIE's workforce (including employees, volunteers, trainees and other persons who, in the performance of work for HIE are under HIE's direct control) shall receive training on HIE's privacy policies and procedures and federal and state laws concerning PHI. Such training should be conducted as necessary and appropriate for HIE's workforce members to carry out the workforce members' duties for HIE. HIE workforce members whose responsibilities include developing, conducting, or monitoring workforce training shall be familiar with this Policy and shall follow these procedures.

TEXAS LAW ANALYSIS:

Texas Health and Safety Code Section 181.101, as added by H.B. 300 (82R), is more narrowly tailored than HIPAA in that it applies only to employees of the Texas Covered Entity rather than the Texas Covered Entity's workforce as a whole and specifically requires training to be customized to each employee's scope of employment. S.B. 1609 (83R) amended Section 181.101. Additionally, Texas law provides a deadline by which initial training must be conducted for new hires (within 90 days), requires follow-up training to be conducted within a reasonable period (not to exceed one year from the effective date of the new law) if the duties of a workforce member are affected by a material change in state or federal law concerning PHI; and requires the Texas Covered Entity to maintain a signed certification from the employee stating that he or she has received the required training for a period of six years. To facilitate compliance with federal and state law, this Policy applies the additional requirements of Texas privacy law to all workforce members -- and not just employees -- of HIE.

PROCEDURE

NOTE: The training requirements under both the Privacy Standards or Security Standards and the Texas Medical Records Privacy Act are flexible and scalable depending on the size of the Texas Covered Entity. Accordingly, a large entity may choose to provide training programs with classroom instruction, video presentations and interactive software. By contrast, a small entity may provide members of its workforce a copy of the entity's privacy policies and procedures and require its workforce members to acknowledge that they have read, reviewed and understand such policies. The content of the training program shall depend on the members of the workforce being trained; however, all workforce members must be trained on the recognition and reporting of privacy violations to the appropriate responsible person for the entity. Certain workforce members may require additional or more in-depth training than others depending on the amount of contact they have with PHI in the course of their duties.

1. Training Required. HIE shall have a policy requiring its individual workforce members to attend scheduled training conducted or provided by HIE. HIE may want to consider instituting disciplinary action against a workforce member for failure to attend required training. Training shall include training with respect to potential penalties for failure to

comply with HIPAA and Texas privacy laws, including civil monetary penalties of up to $50,000 per violation and criminal punishment.

2. Role-Based Training. The training received by a workforce member should be provided as necessary and appropriate for the workforce members to carry out the workforce members' duties for HIE.

3. Responsibility for Training. HIE shall designate an individual, an office or department within its organization with responsibility for training its workforce members regarding federal and state laws concerning PHI and its own privacy policies and procedures. Such training may include:

   a. developing standardized methods and materials to provide privacy training, including a "train-the-trainer" approach whereby an instructor who is an expert in HIPAA privacy requirements conducts the initial training for the privacy officer, department managers or supervisors, privacy committee members and others who shall be involved in privacy training;

   b. identifying appropriate personnel and assigning responsibility for privacy awareness and training;

   c. conducting all privacy training sessions for workforce members;

   d. ensuring that current policies and procedures are addressed at staff meetings periodically;

   e. ensuring that the training includes role-playing, case studies, seminars and discussions, in addition to traditional lectures, video presentations or interactive software programs;

   f. maintaining all documentation of training; and

   g. developing competency tests to evaluate training effectiveness.

4. Initial Training. HIE shall ensure that new workforce members receive training within a reasonable period of time (e.g., three days) but no later than 90 days after the person joins HIE's workforce and before the employee shall be allowed to use or disclose PHI without direct supervision. Privacy policies and procedures shall be included in any orientation information packet provided to new employees, trainees, volunteers and vendors.

5. Additional Training. HIE shall provide additional training in the event of a material change in state or federal medical privacy law concerning PHI or HIE's privacy policies and procedures. Those workforce members whose functions are affected by the material change must complete additional training within a reasonable period of time (e.g., one month), but no later than one year after the material change becomes effective.

6. Documentation. HIE shall maintain in written or electronic form a workforce training log documenting workforce members' completion of privacy training. See Appendix B for a sample workforce training log. Training records must be kept for at least six years from the date of their creation. Further, HIE shall require each employee who attends a training session to certify, either electronically or in writing, that the employee attended and received the required training. HIE shall maintain the signed statement for its records for at least six years. HIE may also consider placing a copy of a workforce member's training documentation in such member's personnel file.

   A Workforce Member Health Information Confidentiality Agreement is also provided at Appendix C as an additional avenue for compliance. New workforce members can be asked to sign this statement of confidentiality prior to the compliance deadline at the beginning of his or her employment in which the workforce member attests that he or she is aware of and understands HIE's policies and procedures and has completed privacy training.

REFERENCES/CITATIONS

45 C.F.R. §§ 164.530(b), (j)

65 Fed. Reg. 82462, 82561, 82745-46, 82755-56, 82770, 82783 (Dec. 28, 2000); 67 Fed. Reg. 53182, 53253 (Aug. 14, 2002)

TEX. HEALTH & SAFETY CODE § 181.101, as added by HB 300 (82R), and amended by SB 1609 (83R).

ARTICLE XII - RECEIVING AND RESOLVING COMPLAINTS

POLICY

HIE may have a process by which any person can make a complaint to HIE or the Secretary regarding HIE's privacy policies, procedures, and/or practices, as well as, HIE's compliance with its privacy policies and procedures and the Privacy Standards and Security Standards. However, if HIE develops a process for complaints to the Secretary, then that process must be consistent with 45 C.F.R.160.306. HIE may require its employees, whose responsibilities include receiving and/or responding to complaints, to be familiar with, and follow, the procedures set forth in this Article XII.

PROCEDURE

1. Designation of Contact Person. HIE may allow the designation of a Contact Person for all complaints (such as by the Privacy Officer in accord with Article III of these Model Privacy Policies). HIE may require the Contact Person to be responsible for receiving complaints relating to: (a) privacy policies, procedures, and/or practices; (b) compliance with its policies and procedures; and/or (c) compliance with the Privacy Standards or Security Standards.

2. Inform Persons of Their Right To Complain. HIE will inform persons that they may complain to HIE and/or to the Secretary if they believe their privacy rights have been violated.

3. Filing a Complaint. HIE may provide the following assistance when a person wishes to file a complaint:

    a. Complaints to HIE. If a person (including, but not limited to, a patient, employee, Business Associate, independent contractor, accrediting organization, advocacy agency, or other person, association, group, or organization) wishes to complain to HIE, the person may contact or may be directed to the Contact Person. The Contact Person, or his or her designee, may ask the person whether he or she wishes to submit a written or oral complaint.

        i. Written complaints. If the person wishes to submit a written complaint, the person may be requested to complete their respective organization's complaint form, state in clear terms the nature of the complaint, and/or provide any other information necessary to enable HIE to investigate, review, and resolve the complaint. A sample Complaint form is attached as Appendix D. The Contact Person, or his or her designee, may ensure that the person has filled out the complaint form completely and has provided sufficient information to enable the respective organization to investigate, review, and resolve the complaint.

        ii. Oral complaints. If the person wishes to submit an oral complaint, the Contact Person, or his or her designee, may ask the person to explain the

complaint in sufficient terms to enable the Contact Person to investigate, review, and resolve the complaint. The Contact Person, or his or her designee, may document the oral complaint in writing.

b. Complaints to HHS. If a person wishes to complain to the Secretary, the person shall be provided with information sufficient to make a written complaint, either in paper or electronic form. The complaint must name the respective organization and describe the acts or omissions believed to be in violation of the Privacy Standards or Security Standards. It shall be filed within one-hundred and eighty (180) days of when the person knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown, at one of the following addresses:

Region VI, Office for Civil Rights
United States Department of Health and Human Services
1301 Young Street, Suite 1169
Dallas, TX 75202
Phone: (214) 767-4056
FAX: (214) 767-0432
TDD: (214) 767-8940
e-mail: OCRComplaint@hhs.gov

4. Report to Participant and HIE Management. The Contact Person shall forward all written and oral privacy complaints to the applicable Participant and HIE Management.

5. Investigation and Privilege of Privacy Complaints. The Contact Person may address and resolve all complaints under the direction and supervision of the appropriate committee that addresses all such matters as part of its quality review activities, except that the Secretary will investigate any compliant when a preliminary review of the facts suggest a possible violation due to willful neglect. All such matters may be privileged and confidential under state peer review privilege statutes. The Contact Person, or his or her designee, may investigate and handle as a quality review matter all complaints submitted pursuant to Paragraph 3 of this Policy XI including, as appropriate, interviewing or otherwise contacting other persons involved in the circumstances upon which the complaint is based, and may take all other steps necessary to review and investigate the complaint. Following the completion of the investigation, the Contact Person may make a determination regarding whether any of the following have occurred: (a) member(s) of the respective organization's workforce failed to comply with privacy policies and procedures; (b) member(s) of the workforce failed to comply with the Privacy Standards or Security Standards; or (c) the respective organization's privacy policies, procedures, and/or practices fail to comply with the Privacy Standards or Security Standards. The Contact Person may enlist the help of the Privacy Officer in order to make this determination.

6. Referral of Workforce Members for Sanctions To the extent the Contact Person determines that one or more members of HIE's workforce has failed to comply with the

privacy policies and procedures and/or the Privacy Standards or Security Standards, the Contact Person may refer the respective organization's workforce member(s) to **[name of person or office responsible for sanctioning workforce members]** for sanctions. HIE shall apply appropriate sanctions to the workforce member(s) in accordance with Article XIII of these Model Privacy Policies.

7. Resolution of Privacy Complaints. The Contact Person may, within **[a reasonable period of time (state time period)]**, provide the complaining person with written notice of the decision regarding the complaint that includes: (a) the name of the individual handling the complaint, if different from the Contact Person; (b) the fact that an investigation has/will take place; (c) the date of completion or expected completion; and (d) notification that due to the confidential and privileged nature of the peer review/quality review process, the results of such proceedings may not be communicated to the person.

8. Complaint Log. The Contact Person may maintain a log documenting privacy complaints received and their disposition, if any. Documentation may be maintained in written or electronic for a specified amount of time.

9. No Intimidating or Retaliatory Acts. HIE may require Participant to prohibit any member of Participant's workforce from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against an individual for the exercise by that individual of any right under the Privacy Standards or Security Standards, or for participation by the individual in any process established by the Privacy Standards or Security Standards. This requirement may apply to any individual filing a complaint with the Secretary; testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing arising under the Privacy Standards or Security Standards; or opposing any act or practice of the respective organization, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not disclose PHI in violation of the Privacy Standards or Security Standards.

10. No Waiver of Rights. HIE may require of Participants that no person shall be asked to waive his or her rights, including the right to file a complaint with the Secretary, as a condition of treatment or payment.

REFERENCES/CITATIONS

Business Associate: 45 C.F.R. § 160.306

Covered Entity: 45 C.F.R. 164.520(b)(vi); 164.530(a), (b), (d), (g), (h)

42 C.F.R. § 482.13(a)(2) (2001) (Medicare Conditions of Participation)

65 Fed. Reg. 82462, 82487, 82550, 82562, 82563, 82600-01, 82746-47, 82748, 82768, 82783, 82801-02, 82821, 82826-28 (Dec. 28, 2000); 67 Fed. Reg. 53182-273 (Aug. 14, 2002); 68 Fed. Reg. 13711-12

78 Fed. Reg. 5578-79 (Jan. 25, 2013)

ARTICLE XIII - SANCTIONS

POLICY

HIE shall have and apply appropriate sanctions against members of its workforce who fail to comply with the requirements under these Model Privacy Policies or the Privacy Standards or Security Standards.

PROCEDURE

1. Parties Responsible for Imposing Discipline. Identify the persons or committees that will be responsible for determining sanctions for privacy violations. The identified parties should have sufficient knowledge of the Privacy Standards or Security Standards and sufficient authority to back their disciplinary determinations. It may be preferable to select parties other than the Privacy Officer, so that the Privacy Officer can independently review the parties' determinations and actions.

2. Persons Who May Be Subject to Discipline. Members of HIE's workforce, including employees, volunteers, trainees, and other persons whose conduct, in the performance of their work, is under HIE's direct control (control is determined using the federal common law of agency)[3], whether or not they are paid by HIE, may be subject to discipline under this Article XIII. Independent contractors are considered HIE's Business Associates, not members of HIE's workforce, and are not subject to discipline under this Article XIII.

3. Violations That Will Prompt Consideration of Disciplinary Action. HIE may impose discipline, up to and including discharge and/or restitution, for violations of either these Model Privacy Policies or the Privacy Standards or Security Standards or other applicable law. Managers or supervisors may also be subject to discipline, up to and including discharge or restitution, if their lack of diligence, or lack of supervision, contributes to a privacy violation.

4. Exceptions. HIE shall not impose discipline as a result of performing one or more of the following:

    a. Filing a complaint with the Secretary for a suspected violation of the Privacy Standards or Security Standards;

    b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing in connection with the Administrative Simplification provisions of HIPAA;

    c. Opposing any act or practice made unlawful by the Privacy Standards or Security Standards, provided that (i) the person has a good faith belief that the practice opposed is unlawful and (ii) the manner of the opposition is reasonable and does

[3] 78 Fed Reg. 17, 5580.

not involve a disclosure of PHI in violation of the Privacy Standards or Security Standards; or

d. Disclosing PHI if (i) the person believes in good faith either that the HIE has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by his or her respective organization potentially endanger one or more patients, workers, or the public; and (ii) the disclosure is either to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the respective organization, to an attorney retained by or on behalf of the person for the purpose of determining the person's legal options with regard to the relevant conduct, or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct.

5. Imposition of Discipline. If warranted, HIE shall impose discipline that is appropriate to the nature of the violation that prompted the disciplinary action. Determination of the proper level of disciplinary action requires that the facts and circumstances surrounding the violation be considered. After considering the relevant facts and circumstances of a privacy violation, HIE shall impose discipline that it deems appropriate, in its sole discretion, to the nature of the violation that prompted the disciplinary action. Discipline may include, but is not limited to, a fine, probation, suspension, additional training, and/or termination.

6. Enforcement of Discipline. HIE shall ensure that the imposed discipline is adequately communicated to the violator and enforced. In the event that the discipline triggers any rights of appeal (for instance, under a collective bargaining agreement), all such rights of appeal shall be available to the violator. However, in the event that the party hearing the appeal is not a party authorized in Paragraph 1 of this Article XIII to impose discipline, the identity of the individual whose privacy rights were violated shall be removed to the extent feasible.

7. Documentation of Discipline. HIE shall document, and shall also require its Participants to document, the disciplinary action, including (a) the privacy violation, (b) the parties that determined the action, (c) the facts and circumstances considered in determining the action (without regard to whether such considerations were relied upon in determining the disciplinary action), (d) the discipline imposed (including lack of discipline), (e) the appeals process used, if any, and the results thereof, and (f) the actions taken in order to enforce the discipline.

HIE shall maintain the documentation described in the above paragraph for a period of at least six (6) years from the date it was created.

HIE may use or disclose its documentation containing the identity of the individual whose privacy rights were violated only under the following circumstances:

a. if required by law or by court order;

b. in accordance with the individual's authorization;

c. in determining disciplinary actions for subsequent violations; or

d. to investigate or determine compliance with these Model Privacy Policies and/or the Privacy Standards or Security Standards (whether such investigation originates internally or by request of the individual or the Secretary).

Under any other circumstances, such documentation must be de-identified (as to the individual whose privacy rights were violated) prior to any use or disclosure. For example, documentation of disciplinary actions, if de-identified, may be stored in the violator's personnel file. In addition, where feasible, the violator's identity should be removed prior to any use or disclosure, for example if the documentation is to be used by those responsible for privacy training.

REFERENCES/CITATIONS

45 C.F.R. §§ 164.502(j), 164.530(e), (g)(2) (2013)

65 Fed. Reg. 82462, 82501-02, 82562, 82636-37, 82747 (Dec. 28, 2000), 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

ARTICLE XIV - MITIGATION

POLICY

HIE shall mitigate any harmful effect known to HIE of a use or disclosure of PHI by HIE or any of its subcontractors in violation of the Privacy Standards or Security Standards. Employees of HIE, who are responsible for mitigating the harmful effect of any inappropriate uses or disclosures, shall be familiar with, and follow, the procedures set forth in this Article XIV. The HIE should consult its BAAs and Participation Agreements with its Participants to ensure there are not additional requirements regarding mitigation and shall reasonably cooperate in their efforts to mitigate. Any additional requirements from the BAA must be included in any BAA with a subcontract of HIE.

TEXAS LAW ANALYSIS:

Sections 181.201 - 181.206 of the Texas Health and Safety Code impose higher penalties than HIPAA for privacy violations of PHI and also allow for enforcement and disciplinary action by a greater number of agencies.

PROCEDURE

1. Report Harmful Effects of Inappropriate Uses or Disclosures to the Privacy Officer. A workforce member of HIE who knows of a harmful effect of a use or disclosure of PHI that is believed to violate the Privacy Standards or Security Standards shall report the use or disclosure, and any relevant facts surrounding the use or disclosure, to the Privacy Officer or other appointee responsible for collecting such reports.

2. Establish Duty to Mitigate. If HIE's Privacy Officer, or other appointee, determines that HIE knows of a harmful effect of a use or disclosure of PHI that is in violation of the Privacy Standards or Security Standards, HIE shall mitigate, to the extent practicable, the harmful effect. The duty to mitigate applies only if: (a) HIE has actual knowledge of the harm; and (b) mitigation is practicable. Please note that HIE is not required to eliminate the harm unless eliminating the harm is practicable.

3. Take Reasonable Steps to Mitigate Harmful Effects. HIE shall take reasonable steps to mitigate a known harmful effect of a use or disclosure of PHI by HIE. The reasonable steps may be implemented based on HIE's prudent judgment, including, without limitation, HIE's knowledge of: (a) to whom the information has been disclosed; (b) how the information might be used to cause harm to the patient or another individual; and (c) what steps can actually have a mitigating effect with respect to the particular situation.

4. Mitigation Relating to Subcontractors. HIE is not required to monitor the activities of its subcontractors; however, if HIE knows of a pattern of activity or practice of a subcontractor that constitutes a material breach or violation of the subcontractor's obligation under the subcontractor contract, or other arrangement, HIE shall take

reasonable steps to cure the breach or end the violation, as applicable and, if such steps are unsuccessful:

a. Terminate the BAA or arrangement, if feasible; or

b. If termination is not feasible, HIE shall report the problem to the Secretary.

REFERENCES/CITATIONS

45 C.F.R. §§ 164.504(e); 164.530(f)

65 Fed. Reg. 82462, 82562-63 (Dec. 28, 2000), 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

78 Fed. Reg. 5599-5601 (Jan. 25, 2013)

ARTICLE XV - PARTICIPANT AND SUBCONTRACTOR BUSINESS ASSOCIATE AGREEMENT POLICY

POLICY

Because HIE is a Business Associate of its Participants who are Covered Entities, HIE must enter into a Business Associate Agreement with each of its Participants. HIE should not receive any PHI from a Participant until a fully executed BAA has been entered into between the parties. Additionally, HIE shall enter into a business associate agreement with any subcontractor that HIE delegates a function, activity, or service, other than in the capacity of a workforce member of the HIE, that involves the creation, receipt, maintenance, or transmission of PHI.

Editor's Note: Based on the HIE's model, HIE may or may not maintain PHI in a designated record set. This article addresses one or more issues regarding HIEs that do maintain PHI in a designated record set. For those HIEs that do not maintain PHI in a designated record set, this article may be modified according to the model utilized by that HIE.

PROCEDURE

1. Participant Business Associate Agreements. HIE shall enter into a BAA with each of its Participants. A model BAA form that was provided to the local HIEs in March of 2012 and has since been updated to reflect current law under the HIPAA Omnibus Rule is attached hereto as Appendix A. HIEs might keep in mind that to the extent that they negotiate individual terms with individual Participants, this may result in the creation of various, different obligations on the part of the HIE.

2. Subcontractor Business Associate Agreements. HIE shall enter into a Business Associate Agreement with any entity that receives PHI from HIE and performs a function on behalf of the HIE.

    a. *Responsibility for Uses and Disclosures by Subcontractors*. Routine uses and disclosures by subcontractors must be reviewed and appropriate business associate contracts or amendments negotiated. Following execution of business associate contracts or amendments with a subcontractor, a copy of the contract or amendments shall be routed to HIE's Contact Person. Any non-routine use or disclosure by a subcontractor that is either reported by the subcontractor or discovered by HIE personnel must be reported to the HIE Contact Person immediately. HIE must ensure that any limitations put on its uses and disclosures by its BAA with Participant is included in its BAA with any subcontractors.

    b. *Identify Subcontractors who access Protected Health Information*. HIE must identify all of its subcontractors who receive, access or otherwise use for process PHI on behalf of HIE.

c. *Subcontractor's Obligations*. The subcontractor should be able to demonstrate to HIE that it has procedures in place to assure that it can adequately safeguard PHI. The subcontractor must be able to assist HIE in a timely manner whenever one of HIE's Participant's patients seeks to exercise his or her privacy rights regarding health information that is maintained by the subcontractor. This includes the ability to do the following:

i. Provide the patient with copies or access to any PHI about the patient that the subcontractor maintains in a "designated record set," upon request of HIE's Participant.

ii. Amend any protected health information about the patient that the subcontractor maintains in a designated record set, upon request of HIE's Participant.

iii. Maintain an accounting of all disclosures for purposes other than for treatment, payment, and health care operations, and provide the accounting upon request of HIE's Participant.

iv. Comply with all of HIE's Participant's requests regarding confidential communications and restrictions on the use and disclosure of PHI.

NOTE: If the subcontractor does not maintain PHI about patients in a designated record set, the subcontractor Business Associate Agreement does not have to include provisions requiring the subcontractor to allow the patient to inspect or amend such information.

d. *Notification to Subcontractor*. HIE should notify its subcontractors in writing whenever it changes its policies or procedures in a manner that affects the subcontractor. Document the name of the person notified and the date when the subcontractor was notified of the change.

e. *Minimum Necessary Disclosures*. All disclosures to subcontractors must be limited to the minimum amount of information needed for the subcontractor to carry out its functions on behalf of HIE, unless an exception to the minimum necessary rule applies by law and pursuant to HIE's policies.

f. *Violations by Subcontractor*. If HIE learns, or has reason to believe, that the subcontractor is in violation of the business associate agreement, or is in any way jeopardizing the privacy and confidentiality of HIE's Participant's information, the subcontractor must be notified immediately to cease such activities.

i. If the violation is not remedied, the agreement with the subcontractor must be terminated. A reasonable cure period may be allowed.

ii. If termination is not feasible because the subcontractor is the only qualified and available vendor for such services, the Compliance Officer

must notify the Secretary of Health and Human Services of the problem, and shall continue to seek to require the subcontractor to remedy the violations.

g. *Termination of Business Associate Agreement with a Subcontractor*. If the business associate agreement is terminated for any reason, the subcontractor must do the following:

i. Return all PHI still in its possession, or assure that the information is properly destroyed in a manner that protects the confidentiality of the information. The subcontractor must provide a certificate of destruction showing that the information has been properly destroyed.

ii. If any of the information cannot be returned or destroyed (for example, because the subcontractor is required maintain certain information for inspection by regulatory agencies), the subcontractor may retain the information as long as it continues to protect the information in accordance with the terms of the subcontractor information and to use the information only for the purposes that make return or destruction infeasible.

h. *Documentation*. This version of the policy, together with any forms and other documentation obtained in accordance with the policy, shall be retained for a minimum of six years.

45 C.F.R. §§ 164.502(e), 164.504(e)

78 Fed. Reg. 5573 (Jan. 25, 2013) (Definition of subcontractor)

ARTICLE XVI - DOCUMENTATION, AMENDMENT AND RETENTION OF RECORDS POLICY

POLICY

HIE shall document and retain, and may also require its Participants to document and retain, policies and procedures to safeguard the confidentiality of PHI that are reasonably designed to comply with the standards, implementation guidelines, or other requirements of the HIPAA Privacy Standards or Security Standards, as applicable. These policies and procedures shall be amended as necessary to comply with federal and state laws and regulations as well as with the needs and responsibilities of the respective organization.

TEXAS LAW ANALYSIS:

Texas law in several instances provides a longer period of time than HIPAA for which certain records containing PHI are required to be retained by certain health care providers. While these laws are not directly applicable to HIEs (as HIEs are not considered health care providers), HIEs should be aware of Participants' obligations and any retention obligations under their BAAs and Participation Agreements with Participants.

PROCEDURE

1. Documenting Policies and Procedures. HIE shall document (as applicable for those below-listed provisions to an HIE as a business associate), and may also require its Participants to document (as applicable for those below-listed provisions to a Participant as a HIPAA covered entity), policies and procedures related to the following topics in written or electronic form:

    a. Responsibility of the Privacy Officer (optional).

    b. Patient authorization to use or disclose PHI, including:

        i. permission to orally agree or object to the release of certain information; and

        ii. effect of prior consents and authorizations.

    c. Patient rights, including:

        i. notice of privacy practices;

        ii. restrictions on uses and disclosures of PHI;

        iii. request for confidential communications;

        iv. access to inspect and copy records;

v. amendment of records; and

vi. accounting of disclosures.

d. De-identification and re-identification.

e. Minimum necessary standard, including:

i. use of PHI;

ii. routine requests;

iii. non-routine request;

iv. routine disclosures;

v. releasing the entire medical record; and

vi. oral communications.

f. Research.

g. Marketing (optional).

h. Fundraising.

i. Safeguards, including:

i. administrative;

ii. technical; and

iii. physical.

j. Training, including:

i. workforce training;

ii. other educational tools; and

iii. educating patients about their rights and responsibilities.

k. Audits, including:

i. routine internal audits; and

ii. compliance audits by Office for Civil Rights.

l. Receiving and resolving complaints.

m. Sanctions.

n. Mitigation.

o. Agreements with vendors and service providers who are:

i. Business Associates;

ii. trading partners; and

iii. chain of trust partners.

p. Requests for preemption exception.

q. Documentation and record retention.

r. Policy and procedure amendments.

s. Such other topics as the respective organization determines are necessary to comply with the Privacy Standards or Security Standards or to protect the confidentiality of PHI.

HIE shall also assess and document, and may also require its Participants to assess and document, the (a) policies and procedures; (b) communications; and (c) actions, activities, or designations that must be documented to satisfy the express requirements of, or to otherwise ensure compliance with, the Privacy Standards or Security Standards.

2. Amendment of Policies and Procedures. HIE shall formulate, adopt, and recommend, and may also require its Participants to formulate, adopt, and recommend, changes and amendments to these policies and procedures as necessary to improve confidentiality practices or in response to changes in state or federal laws or regulations.

a. *Initiation of Amendments*. HIE may place the initial responsibility and authority with the Privacy Officer, or some other person appointee, to formulate, adopt, and recommend any changes and amendments to the privacy policies and procedures in these Model Privacy Policies, or to add policies and procedures as necessary or required by law or regulation. HIE may require that the responsibility to propose and adopt be exercised in a timely and responsible manner, reflecting the interests of providing patient privacy and confidentiality commensurate with state and federal law, rules and regulations, and standards applicable to accrediting agencies.

b. *Process for Amendment*. To the extent permitted by its BAA and Participation Agreement, HIE may amend the respective policies and procedures at any time. If an amendment is being adopted to implement a requirement of any state or federal regulation, or the requirements of an accrediting entity or governmental agency with jurisdiction over that organization, HIE should require such amendment to be

performed in as timely a manner as necessary. Adoption of amendments to this Model Privacy Policy may be effected in the same manner required for adoption of other HIE policies. If HIE makes any representations to consumers about its policies, and particularly any representations regarding how PHI is used, HIE should ensure that it has reserved the right to make changes, and otherwise provide effective notice of any changes to its policies that affect consumers.

c. *Effect on Notice of Privacy Practice* When HIE amends a policy and procedure that affects the confidentiality of PHI, it should consider to what extent Participants will in turn need to amend their Notices of Privacy Practices. Note that with respect to uses of PHI received prior to the modification of the Notice of Privacy Practices, in order to permit retroactive application of the revisions, the Covered Entity must have reserved the right to make such retroactive revisions through a statement in its Notice of Privacy Practices.

d. *Documentation of Amendment*. HIE shall document all amendments to their policies and procedures.

e. *Review (Optional)*. These Model Privacy Policies shall be reviewed at least **[annually, biannually, or some other length of time]** to determine compliance with applicable laws, regulations, and accreditation standards.

3. Effective Date of Revisions to Policies and Procedures. Revisions to privacy policies and procedures shall become effective when they are: (a) documented; (b) compliant with the standards, requirements, and implementation specifications of the Privacy Standards or Security Standards; and (c) adopted in the manner required by HIE.

4. Retention of Documents Demonstrating Privacy Compliance. HIE shall retain, and may also require its Participants to retain, the policies and procedures provided for in this Article XVI and any other communications, activities, or designations required by the Privacy Standards or Security Standards to be documented for a certain specified period of time.

5. Retention of Medical Records . HIE shall retain PHI for reasonable time periods to ensure that its Participants will be able to comply with applicable law.

REFERENCES/CITATIONS

HITECH § 13405

45 C.F.R. §§ 164.520(b)(1)(v)(C), 164.530(i), 164.530(j) (2013)

65 Fed. Reg. 82462, 82563 (Dec. 28, 2000), 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

ARTICLE XVII - BREACH NOTIFICATION POLICY

POLICY

The Breach Notification for Unsecured Protected Health Information Rule requires Covered Entities, such as Participants, to notify individuals and HHS when a breach of such individual's PHI has occurred. The HIE, as a Business Associate of the Participant, must notify the Participant in a timely manner in order for the Participant to notify the individual and HHS. The Participant may also delegate Breach Notification to the HIE in the BAA. HIE shall consult its Participant BAA and Participation Agreement to determine whether they contain any more specific requirements regarding breaches.

When multiple Participants take part in HIE and there is a breach of unsecured PHI at the HIE, the obligation to notify individuals of the breach falls to the Participants (as the Participants are HIPAA covered entities). In this situation, it may be difficult to determine what breached information is attributable to which Participant's individuals. For example, HIE may store centralized EHRs for a community, with each EHR including information generated by multiple Participants. In such circumstances, it may be necessary for HIE to notify all potentially affected Participants and for those Participants to delegate to HIE the responsibility of sending the required notifications to the affected individuals. This may avoid the confusion of individuals receiving more than one notification of the same breach. This process will depend on HIE's model, and will be dictated by the terms of the BAA between HIE and its Participants.

Editor's Note: The HIPAA/HITECH Final Omnibus Rule replaces the "harm" standard with an analysis of "whether the PHI has been compromised" when addressing a potential breach. However, this does not mean that HIE should disregard any potential harm to the individual who is the subject of the breach. If the breach results in a violation of HIPAA or the Texas Medical Records Privacy Act, then when determining the amount of the penalty, the Secretary (for HIPAA violations) or the court (for Texas Medical Record Privacy Act violations) must consider the financial, reputational, or other harm to an individual whose PHI is involved in the violation. This information may also be presented as mitigating evidence in an action or proceeding to impose an administrative or civil penalty.

PROCEDURE

1. Definitions.

    a. *Breach*. The term "breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Standards or Security Standards which compromises the security or privacy of PHI. Any acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy and Security Standards is presumed to be a breach unless the Participant or HIE can show a low probability that the PHI has been compromised based on the following factors: the nature and extent of the PHI including the types of identifiers and likelihood of re-identification; the unauthorized person who used the PHI or to

whom the disclosure was made; whether the PHI was actually acquired or viewed; and the extent to which the risk has been mitigated.

Breach excludes:

i. Any unintentional acquisition, access, or use of PHI by a workforce member, person acting under the authority of HIE, Participant, or a Business Associate of HIE or Participant, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Standards or Security Standards.

ii. Any inadvertent disclosure by a person affiliated, either directly or indirectly, with HIE or Participant, including a Business Associate, who is authorized to access PHI, to another person authorized to access PHI that is affiliated, either directly or indirectly, with HIE or Participant, including a Business Associate, or to an organized health care arrangement in which HIE or its Participant participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the. Privacy Standards or Security Standards.

iii. A disclosure of PHI where HIE or Participant, or a Business Associate of HIE or Participant, has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

b. *Unsecured PHI*. The term "unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under Section 13402(h)(2) of Pub. L. 111-5 on the HHS web site.

2. Breach Notification Requirements for a Business Associate.

a. The rule regarding breach notification for unsecured PHI requires covered entities, such as Participants, to notify individuals and HHS when a breach of such individual's unsecured PHI has occurred. Business Associates, such as HIEs, must notify the covered entity or Participant of the breach. HIE shall notify Participant, without unreasonable delay, following the discovery of a breach of unsecured PHI, in accordance with any timeframes set forth in the applicable BAA and/or Participation Agreement, but in no case later than sixty (60) calendar days after discovery of the breach. HIE shall consult with legal counsel to determine whether a breach has occurred or whether it is subject to any of the exceptions in Section 1(a)(i)-(iii) above.

b. A breach shall be treated as discovered by HIE as of the first (1st) day on which such breach is actually known to HIE or, by the exercise of reasonable diligence, would have been known to HIE. HIE shall be deemed to have knowledge of a breach if the breach is actually known, or by the exercise of reasonable diligence, would have been known to any reasonably prudent person, other than the person committing the breach, who is in the position of an employee, officer, or other agent of HIE.

c. The notification should include sufficient information to understand the nature of the breach. For instance, such notification could include, to the extent available at the time of the notification, the following information:

i. One or two sentence description of the breach;

ii. Description of the roles of the people involved in the breach (e.g. employees, Participants, service providers, unauthorized persons, etc.);

iii. The type of unsecured PHI breached;

iv. Participants likely impacted by the breach;

v. Number of individuals or records impacted/estimated to be impacted by the breach;

vi. Actions taken by HIE to mitigate the breach;

vii. Current Status of the breach (e.g., under investigation or resolved);

viii. Corrective action taken and steps planned to be taken to prevent a similar breach.

ix. The identification of each individual whose unsecured PHI has been, or is reasonably believed by HIE to have been, accessed, acquired, used, or disclosed during the breach.

d. HIE shall supplement the information contained in the notification as it becomes available. The notification required by this Policy shall not include any PHI. If, on the basis of the notification, Participant desires to stop transacting PHI with HIE, it shall stop transacting PHI in accordance with these policies.

e. HIE and Participants may enter into an agreement that modifies the requirements outlined here in Paragraph 2, including, but not limited to, an agreement to shorten the timeframe for notification by HIE required by paragraph 2 or an agreement to require HIE to notify affected individuals on behalf of Participant in the event that a breach of unsecured PHI is discovered by HIE.

3. Breach Detection and Analysis.

a. HIE may develop, implement, and maintain processes for detecting, managing, and responding to suspected or confirmed breaches of protected health information.

b. As soon as a breach is suspected or has been identified, the workforce member or agent of HIE who discovers the breach must take immediate steps to report the breach to _____. **[Note: Depending on HIE's specific circumstances and preferences, the entity may want the breach reported to a specific committee, supervisor or other individual tasked with handling breach situations.]**

c. Upon receipt of such a report, the Contact Person shall gather information, investigate and determine whether a breach has occurred. The following questions should be addressed during this analysis:

   i. Has there been an impermissible use or disclosure of an individual's protected health information under the Privacy Standards or Security Standards?

   ii. Does the impermissible use or disclosure pose a risk that the individual's PHI has been compromised? (See subsection "d" below for further analysis)

   iii. Do any of the exceptions to the definition of "breach" apply?

   iv. Is the protected health information at issue considered "unsecured protected health information"?

d. Assessment of probability that PHI has been compromised.

When conducting an assessment of the probability that PHI has been compromised, HIE should consider at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

To assess this factor, HIE should consider the type of PHI involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature. With respect to financial information, this may include credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. With respect to clinical information, this may involve considering not only the nature of the services or other information, but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results, etc.).

In situations where there are few, if any, direct identifiers in the information impermissibly used or disclosed, HIE should determine whether there is a likelihood that the PHI released could be re-identified based on the context and the ability to link the information with other available information.

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

HIE should consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information. For example, if the PHI is impermissibly disclosed to another entity required to abide by the HIPAA Privacy and Security Rules or to a Federal agency obligated to comply with the Privacy Act of 1974 and the Federal Information Security Management Act of 2002, there may be a lower probability that the PHI has been compromised because the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as HIE.

This factor should also be considered in combination with the first factor discussed above regarding the risk of re-identification. If information used or disclosed is not immediately identifiable, HIE should determine whether the unauthorized person who received the PHI has the ability to re-identify the information.

iii. Whether the PHI was actually acquired or viewed; and

HIE should investigate an impermissible use or disclosure to determine whether the PHI was actually acquired or viewed, or alternatively, if only the opportunity existed for the information to be acquired or viewed. For example, if a laptop computer was stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, HIE could determine that the information was not actually acquired by an individual even though the opportunity existed. In contrast, however, if HIE sent the information to the wrong individual who called HIE and told HIE that the individual had viewed the information in error, then, in this case, the unauthorized recipient viewed and acquired the information because she actually opened and read the information.

iv. The extent to which the risk to the PHI has been mitigated.

HIE should attempt to mitigate the risks to PHI following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be

destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.

Other factors may also be considered where necessary. If an evaluation of these factors fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required. However, HIE does have the discretion to provide the required notification following an impermissible use or disclosure of PHI without performing a risk assessment.

This analysis shall be documented in writing and retained for a period of 6 years.

4. Administrative requirements.

a. *Training*. HIE shall train all members of its workforce as necessary and appropriate to ensure HIE's compliance with this Article XVII in accordance with Article XI of these Model Privacy Policies.

b. *Sanctions*. HIE shall apply appropriate sanctions, in accordance with Article XIII, against members of its workforce that fail to comply with this Article XVII.

c. *Complaints*. Individuals can make complaints concerning this Article XVII in accordance with Article XII of these Model Privacy Policies.

d. *Documentation*. HIE shall comply with Article XVII of these Model Privacy Policies and shall document that all notifications are made in accordance with applicable law and these Model Privacy Policies and retain any findings or other records regarding the respective organization's determination that a particular use or disclosure does or does not constitute a breach.

REFERENCES/CITATIONS

45 C.F.R. §§ 164.400–414; 164.530(b), (d), (e), (g), (h), (i), (j).

Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009).

Modifications to the Breach Notification Rule Under the HITECH Act, 78 Fed. Reg. 5638-44, 5651 (Jan. 25, 2013)

Pub. L. 111-5, div. A, title XIII, § 13402, Feb. 17, 2009 ("American Recovery and Reinvestment Act of 2009").

Editor's Note Information

TEX. HEALTH & SAFETY CODE §§ 181.201(d)(3) and 181.205(b)(3), as added by H.B. 300 (82R)

45 C.F.R. § 160.408

78 Fed. Reg. 5584-85 (Jan. 25, 2013)

ARTICLE XVIII - SENSITIVE PERSONAL INFORMATION BREACH NOTIFICATION

POLICY

The Texas Identity Theft Enforcement and Protection Act (the "Act") requires any entity in the state that maintains computerized data containing sensitive personal information not owned by the entity to provide notice to the owner or license holder of the information of any breach of system security if the information was, or is reasonably believed to have been, acquired by an unauthorized person. As an entity that maintains computerized data including sensitive personal information, HIE shall develop and maintain processes for detecting, managing, and responding to suspected or confirmed breaches of sensitive personal information and adopt a policy on providing timely and appropriate notice in the event of a system security breach. HIE shall also ensure that its Participants, as entities that own computerized data containing sensitive personal information, have policies in place to comply with the Act.

PROCEDURE

1. Definitions.

   a. *Breach of system security*. The term "breach of system security" means the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of sensitive personal information maintained by an individual, including data that is encrypted if the person accessing the data has the key required to decrypt the data. The term excludes the good faith acquisition of sensitive personal information by an employee or agent of an individual for purposes of such individual, unless the employee or agent uses or discloses the sensitive personal information in an unauthorized manner.

   b. *Sensitive personal information*. The term "sensitive personal information" means:

      i. an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

         (1) social security number;

         (2) driver's license number or government-issued identification number; or

         (3) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

      ii. information that identifies an individual and relates to:

         (1) the physical or mental health or condition of the individual;

(2) the provision of health care to the individual; or

(3) payment for the provision of health care to the individual.

The term does not include any publicly available information lawfully made available to the public from the federal, state or local government.

2. Breach Notification Requirements.

a. *Timing Requirements*. Following the discovery of a breach of system security, HIE shall immediately provide written notice to the Participant. However, the HIE may delay in providing notice if requested by a law enforcement agency that determines that notification would impede a criminal investigation. HIE should document such request in writing. In such event, notification shall be made as soon as the law enforcement agency determines that the notice will not compromise the investigation. HIE shall consult its Participant BAA and Participation Agreement to determine whether they contain any additional requirements.

b. *Resident Location.* If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that has its own breach notification laws, then HIE may provide notice of the breach of system security under that state's law or under this policy.

c. *Methods of Breach Notification.* HIE may give notice of a breach of system security by providing:

i. Written notice at the last known address of the individual;

ii. Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; or

iii. If HIE demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:

(1) Electronic mail, if the person has electronic mail addresses for the affected persons;

(2) Conspicuous posting of the notice on the person's website; or

(3) Notice published in or broadcast on major statewide media.

d. *Deemed Compliance*. If HIE maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under the Act, HIE will be

deemed to have complied with the Act if HIE provides notice in accordance with that policy.

REFERENCES/CITATIONS

TEXAS BUSINESS & COMMERCE CODE §521.002 §521.053, as amended by SB 1609 (83R).

ARTICLE XIX - PERMITTED USES AND DISCLOSURES

SECTION A-1 - SUBJECT TO APPLICABLE BUSINESS ASSOCIATE AND PARTICIPATION AGREEMENTS

POLICY

HIE may only use or disclose the PHI of a Covered Entity to the extent authorized under its BAA and Participation Agreement or as otherwise authorized under applicable law.

PROCEDURE

EACH OF THE PERMITTED USES AND DISCLOSURES OUTLINED IN THIS ARTICLE XIX MAY BE LIMITED BY APPLICABLE BAA AND PARTICIPATION AGREEMENTS ENTERED INTO BY THE HIE. THUS, EACH OTHER SECTION OF ARTICLE XIX IS SUBJECT TO THIS SECTION A-1.

ARTICLE XIX - PERMITTED USES AND DISCLOSURES ALTERNATIVE TO SECTION A-2 BELOW - APPLICATION OF MINIMUM NECESSARY RULE

Editor's Note: Based on the HIE's model, this policy may better fit the HIE's needs in complying with state and federal medical privacy law than Section A-2 of Article XIX below.

POLICY

This policy shall be enforce to limit the use and disclosure of PHI by all HIE workforce members to the minimum amount of information necessary to accomplish their job duties or functions. Further, it shall be used to make reasonable efforts to limit use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose.

PROCEDURE

1. Uses.

    a. HIE will identify:

        i. The persons or classes of persons in its workforce who require access to PHI to carry out their job duties;

        ii. The categories or types of PHI required; and

        iii. The conditions appropriate for such access.

    b. HIE workforce members' access to PHI shall be solely on a "need to know" basis. HIE workforce members' use or disclosure of PHI shall be limited to that PHI needed to perform job responsibilities and duties.

2. Routine or Recurring Requests and Disclosures.

    a. For routine and recurring requests and disclosures, HIE shall develop and implement standard protocols.

    b. Non-routine requests for, and disclosures of, PHI shall be reviewed by the Privacy Officer (if HIE should choose to designate one). HIE shall develop and implement criteria to limit its requests for PHI to the minimum necessary to satisfy the request or accomplish the intended purpose.

3. Reasonable Reliance. HIE shall rely on Participant's request for PHI as the minimum necessary for the intended disclosure.

4. Information Systems. All information systems will be designed, in accordance with HIE's available resources, to meet the minimum necessary provisions of the HIPAA final omnibus rule. HIE shall accomplish this by removing identifiers and removing data fields not necessary to performing the primary purpose of the use or disclosure.

5. HIE's privacy officer (if HIE should choose to designate one) shall determine workforce member access to PHI based on job duties and functions and will document in the workforce member's personnel file. Determination of access shall be based on:

    a. Employees or classes of employees who need access to PHI to carry out their daily functions.

    b. For each class of employee, the category or categories of PHI to which access is required.

6. Generally, PHI used by HIE may be used by HIE workforce members to facilitate exchange of information between Participants for treatment, payment, or healthcare operations of HIE's Participants. PHI may not be disclosed outside of HIE unless such disclosure is made to:

    a. A business associate with whom HIE has a business associate agreement or a Participant with whom HIE has a Participant Agreement; or

    b. As otherwise Required by Law.

SECTION A-2 - APPLICATION OF MINIMUM NECESSARY RULE

POLICY

Unless an exception to the minimum necessary rule applies by law and pursuant to HIE's policies as set forth below, when using, disclosing, or requesting PHI from a Covered Entity, HIE shall make reasonable efforts to limit uses, disclosures or requests to the minimum necessary to accomplish the intended purpose and, when practicable, shall limit the use, disclosure or request to a limited data set of the PHI. HIE shall require its employees whose responsibilities include using, disclosing or requesting PHI to be familiar with this Policy and follow these procedures.

Editor's Note: While the purpose of electronic health information exchange is to provide Participants with *more* data regarding an individual's medical information, HIE should also be aware of HIPAA's "minimum necessary" requirements, and try, to the extent possible in the context of an HIE, to limit use and disclosure of protected health information to the minimum necessary.

PROCEDURE

7. The Minimum Necessary Standard Does Not Apply to the Following:

    a. Disclosures to or requests by a health care provider for treatment;

    b. Uses or disclosures made to the individual;

    c. Uses or disclosures made pursuant to an authorization (see Article V of these Model Privacy Policies);

    d. Disclosures made to the Secretary for purposes of enforcing the HIPAA Privacy Standards or Security Standards;

    e. Uses or disclosures that are required by law to the extent they are limited to the relevant requirements of such law (but not disclosures that are merely permitted by law); and

    f. Uses or disclosures that are required for compliance with any regulation implementing the Administrative Simplification provisions of HIPAA.

8. Release of the Entire Medical Record. For all uses, disclosures, or requests to which the minimum necessary standard applies, HIE shall not use, disclose or request the entire

medical record, unless it can specifically justify the entire medical record as the amount necessary to accomplish the purpose of the use, disclosure or request.

9. Additional Regulations. HHS is expected to promulgate additional regulations for factors to consider in applying the minimum necessary rule but such regulations have not yet been promulgated.

REFERENCES/CITATIONS

HITECH § 13405(b)

45 C.F.R. §§ 164.502(b), 164.514(d) (2013)

65 Fed. Reg. 82462, 82543-45, 82616-17, 82712-16, 82767, 82782-83 (Dec. 28, 2000); 67 Fed. Reg. 53182, 53195-99 (Aug. 14, 2002)

ARTICLE XIX - PERMITTED USES AND DISCLOSURES

SECTION B - TREATMENT PURPOSES

POLICY

HIE may disclose PHI without a patient authorization for the treatment purposes of an individual. HIE employees whose responsibilities include using or disclosing PHI for treatment purposes shall be familiar with this Policy and shall follow the procedures set forth herein.

PROCEDURE

1. Disclosures for Treatment Purposes. HIE may disclose PHI for the treatment activities of individuals without a prior written authorization from the individual who is the subject of the PHI, in accordance with the following:

    a. *Definition of Treatment*. Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

    b. *Definition of Health Care Provider*. A health care provider is a provider of medical or health services who is licensed, certified, or otherwise authorized by Texas law to provide health care, including a hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, physician, physical therapist, occupational therapist, nurse mid-wife, social worker, psychologist, ambulance service, or any other person or organization who furnishes bills, or is paid for health care in the normal course of business.

    c. *Permissible Recipients of PHI*. HIE may disclose an individual's PHI for treatment purposes without authorization in accordance with State and Federal medical privacy law.

2. Minimum Necessary Rule. Disclosures for treatment activities are not subject to the minimum necessary standard.

3. Verification. Prior to any disclosure, the identity of the person requesting PHI and the authority of any such person to have access to PHI must be verified if the person's identity or authority is not known to the person making the disclosure. Knowledge of the person can take the form of a known place of business, address, phone or fax number, as well as a known human being. Documentation, statements, or representations, whether oral or written, from the person requesting the PHI must be obtained when such documentation, statement, or representation is a condition of the disclosure. HIE may

rely on documentation, statements, or representations that, on their face, meet the applicable requirements.

a. *Applicability*. This verification requirement applies to all disclosures of PHI permitted by the Privacy Standards or Security Standards, including disclosures for treatment, payment, or health care operations, where the identity of the recipient is not known to HIE. Routine communications between providers, where existing relationships have been established, do not require special verification procedures.

b. *Verification of Identity*. HIE may rely on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

   i. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

   ii. If the request is in writing, the request is on the appropriate government letterhead; or

   iii. If the disclosure is to a person acting on behalf of a public official (e.g., a public health agency contracting with a nonprofit agency to collect and analyze data), a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

c. *Verification of Authority*. HIE may rely on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

   i. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of the legal authority; or

   ii. If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

d. *Professional Judgment*. The verification requirements set forth above in this Policy are satisfied if HIE exercises professional judgment in making a use or disclosure requiring an opportunity for the individual to agree or to object (e.g., emergency situations), or acts on a good faith belief in making a disclosure to avert a serious threat to health or safety.

e. *Minimum Requirements for Verification*. This Policy does not require a disclosure of PHI if these verification requirements have not been satisfied, nor does this Policy preempt state laws that establish additional verification requirements. Where state law establishes more stringent verification requirements, HIE shall adhere to the more stringent requirements.

f. *Request for Verification of Identity of the Patient*. To prevent name mix-ups, the requesting party should provide additional information about the patient whose information is requested, e.g., date of birth, Social Security number, current address, or a combination of all three, and document the information received.

REFERENCES/CITATIONS

HITECH § 13405(b)

45 C.F.R. §§ 160.103, 164.501, 164.502, 164.506 (2013)

65 Fed. Reg. 82462, 82497-99 (Dec. 28, 2000); 67 Fed. Reg. 53182, 53196-97, 53208-19 (Aug. 14, 2002)

45 C.F.R. § 164.514(h) (2002)

65 Fed. Reg. 82462, 82500, 82524, 82538, 82546-47, 82632, 82682, 82686, 82718-20 (Dec. 28, 2000)

ARTICLE XIX - PERMITTED USES AND DISCLOSURES

SECTION C - PAYMENT PURPOSES

POLICY

HIE may disclose PHI without a patient authorization for the payment purposes of an individual. HIE employees whose responsibilities include using or disclosing PHI for payment purposes shall be familiar with this Policy and shall follow the procedures set forth herein.

PROCEDURE

1. Disclosures for Payment Transactions. HIE may disclose PHI without a prior written authorization from the individual who is the subject of the PHI for the payment activities of such individual.

    a. *Definition of Transactions for Payment Purposes*. Transactions for payment purposes include any activity undertaken by a Covered Entity to obtain reimbursement for the provision of health care, including, but not limited to: (a) determinations of eligibility or coverage, including coordination of benefits or the determination of cost sharing amounts; (b) adjudication or subrogation of health benefit claims; (c) risk adjusting amounts due based on enrollee health status and demographic characteristics; (d) billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing; (e) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (f) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (g) disclosure to consumer reporting agencies of PHI relating to the collection of premiums or reimbursement.

2. Minimum Necessary Rule. When disclosing PHI for payment purposes, HIE shall disclose only the minimum PHI necessary to facilitate payment unless an exception to the minimum necessary rules applies by law and pursuant to HIE's policies.

    a. *Reasonable Reliance*. HIE may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

        i. Making disclosures to public officials, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

        ii. The information is requested by a Covered Entity;

        iii. The information is requested by a professional who is a member of a Covered Entity's workforce or is a Business Associate of the Covered

Entity (e.g., attorneys or accountants) for the purpose of providing professional services to the Covered Entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

iv. Documentation or representations that comply with the applicable requirements for research have been provided by a person requesting the information for research purposes in accordance with Article XIX, Section F of these Model Privacy Policies.

b. *Minimum Necessary Standard*. The amount of PHI that constitutes the minimum necessary shall depend upon the type of payment activity that is being undertaken. HIE may rely on the assertions of a Covered Entity that the amount of information requested to facilitate payment is the minimum amount necessary, but HIE may not rely on the assertions of a private, third party that is not a Covered Entity (e.g., a financial institution or credit card payment system).

c. *Disclosure Beyond That Authorized by This Policy*. To the extent that a particular payment disclosure requires the disclosure of PHI beyond that described in this Policy, such disclosure shall undergo individual review by the Contact Person, unless such disclosure is to a health plan. If such disclosure is to a health plan, the PHI requested may be disclosed if it is reasonable.

d. *Disclosing the Entire Medical Record*. There may be situations where disclosure of the entire medical record other than for treatment by health care providers or as otherwise provided in these Model Privacy Policies shall be necessary, but these disclosures must have a documented justification.

3. Verification. Prior to any disclosure, the identity of the person requesting PHI and the authority of any such person to have access to PHI must be verified if the person's identity or authority is not known to the person making the disclosure. Knowledge of the person can take the form of a known place of business, address, phone or fax number, or appropriate electronic access credentials, as well as a known human being. Documentation, statements, or representations, whether oral or written, from the person requesting the PHI must be obtained when such documentation, statement, or representation is a condition of the disclosure. HIE may rely on documentation, statements, or representations that, on their face, meet the applicable requirements. **(NOTE: If HIE includes "appropriate electronic access credentials" to define "knowledge of the person," then HIE should take additional steps to appropriately define what constitutes "appropriate electronic access credentials" in HIE's policies.)**

a. *Applicability*. This verification requirement applies to all disclosures of PHI permitted by the Privacy Standards or Security Standards, including disclosures for treatment, payment, or health care operations, where the identity of the recipient is not known to HIE. Routine communications between providers,

where existing relationships have been established, do not require special verification procedures.

b. *Verification of Identity*. HIE may rely on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

   i. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

   ii. If the request is in writing, the request is on the appropriate government letterhead; or

   iii. If the disclosure is to a person acting on behalf of a public official (e.g., a public health agency contracting with a nonprofit agency to collect and analyze data), a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

c. *Verification of Authority*. HIE may rely on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

   i. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of the legal authority; or

   ii. If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

d. *Professional Judgment*. The verification requirements set forth above in this Policy are satisfied if HIE exercises professional judgment in making a use or disclosure requiring an opportunity for the individual to agree or to object (e.g., emergency situations), or acts on a good faith belief in making a disclosure to avert a serious threat to health or safety.

e. *Minimum Requirements for Verification*. This Policy does not require a disclosure of PHI if these verification requirements have not been satisfied, nor does this Policy preempt state laws that establish additional verification requirements. Where state law establishes more stringent verification requirements, HIE shall adhere to the more stringent requirements.

f. *Request for Verification of Identity of the Patient*. To prevent name mix-ups, the requesting party should provide additional information about the patient whose

information is requested, e.g., date of birth, Social Security number, current address, or a combination of all three, and document the information received.

REFERENCES/CITATIONS

HITECH § 13405(b)

45 C.F.R. §§ 162.1101-162.1802, 162.514(d)(3)(iii), 164.501, 164.502(a)(1)(ii), 164.506, 164.514(h) (2013)

65 Fed. Reg. 82462, 82495-96, 82498-99, 82500, 82524, 82534-35, 82537, 82538, 82545, 82546-47, 82600, 82613-18, 82630, 82632, 82682, 82686, 82715, 82718-20 (Dec. 28, 2000)

67 Fed. Reg. 53182, 53197, 53198, 53203, 53208-19 (Aug. 14, 2002)

ARTICLE XIX - PERMITTED USES AND DISCLOSURES

SECTION D - HEALTH CARE OPERATIONS

POLICY

HIE may disclose PHI without an authorization for the Health Care Operations of the Participant receiving the information. HIE employees whose responsibilities include using or disclosing PHI for health care operations purposes shall be familiar with this Policy and shall follow the procedures set forth herein. HIE may use or disclose PHI as necessary for the proper management and administration of HIE or to carry out its legal responsibilities, provided that such uses are permitted under federal and state law.

PROCEDURE

1. Disclosures for Health Care Operations. HIE may disclose PHI to a Participant for another Participant's health care operations if the Participant either has or had a relationship with the individual who is the subject of the information, the PHI pertains to that relationship, and the disclosure is for a listed purpose in paragraphs 2(a) and 2(b) of this Policy or for the purpose of health care fraud and abuse detection or compliance. The minimum necessary standard shall apply to the disclosure of PHI for these purposes unless an exception to minimum necessary applies by law and pursuant to HIE's policies.

2. Health Care Operations. Health care operations include the following activities to the extent that the activities are related to the recipient Participant's covered functions:

    a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 C.F.R. 3.20); population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

    b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

    c. Except for prohibited uses and disclosures of genetic information, underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health

care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 C.F.R. § 164.514(g) are met, if applicable;

d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

e. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

f. Business management and general administrative activities of the Participant, including, but not limited to:

i. Management activities relating to implementation of and compliance with the requirements of this subchapter;

ii. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer.

iii. Resolution of internal grievances;

iv. The sale, transfer, merger, or consolidation of all or part of the Participant with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and

v. Consistent with the applicable requirements of the HIPAA Privacy Standards or Security Standards, creating de-identified health information or a limited data set, and fundraising for the benefit of the Participant.

3. Minimum Necessary Rule. When disclosing PHI for a Participant's healthcare operations, HIE shall disclose only the minimum PHI necessary to facilitate such operations unless an exception to minimum necessary applies by law and pursuant to HIE's policies.

a. *Reasonable Reliance*. HIE may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

i. Making disclosures to public officials, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

ii. The information is requested by a Covered Entity;

iii. The information is requested by a professional who is a member of a Covered Entity's workforce or is a Business Associate of the Covered Entity (e.g., attorneys or accountants) for the purpose of providing professional services to the Covered Entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

iv. Documentation or representations that comply with the applicable requirements for research have been provided by a person requesting the information for research purposes in accordance with Article XIX, Section F of these Model Privacy Policies.

4. Verification. Prior to any disclosure, the identity of the person requesting PHI and the authority of any such person to have access to PHI must be verified if the person's identity or authority is not known to the person making the disclosure. Knowledge of the person can take the form of a known place of business, address, phone or fax number, as well as a known human being. Documentation, statements, or representations, whether oral or written, from the person requesting the PHI must be obtained when such documentation, statement, or representation is a condition of the disclosure. HIE may rely on documentation, statements, or representations that, on their face, meet the applicable requirements.

a. *Applicability*. This verification requirement applies to all disclosures of PHI permitted by the Privacy Standards or Security Standards, including disclosures for treatment, payment, or health care operations, where the identity of the recipient is not known to HIE. Routine communications between providers, where existing relationships have been established, do not require special verification procedures.

b. *Verification of Identity*. HIE may rely on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

i. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

ii. If the request is in writing, the request is on the appropriate government letterhead; or

iii. If the disclosure is to a person acting on behalf of a public official (e.g., a public health agency contracting with a nonprofit agency to collect and analyze data), a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

c. *Verification of Authority*. HIE may rely on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

i. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of the legal authority; or

ii. If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

d. *Professional Judgment*. The verification requirements set forth above in this Policy are satisfied if HIE exercises professional judgment in making a use or disclosure requiring an opportunity for the individual to agree or to object (e.g., emergency situations), or acts on a good faith belief in making a disclosure to avert a serious threat to health or safety.

e. *Minimum Requirements for Verification*. This Policy does not require a disclosure of PHI if these verification requirements have not been satisfied, nor does this Policy preempt state laws that establish additional verification requirements. Where state law establishes more stringent verification requirements, HIE shall adhere to the more stringent requirements.

f. *Request for Verification of Identity of the Patient*. To prevent name mix-ups, the requesting party should provide additional information about the patient whose information is requested, e.g., date of birth, Social Security number, current address, or a combination of all three, and document the information received.

5. The HIE may use or disclose PHI as necessary for the proper management and administration of the Business Associate or to carry out its legal responsibilities, provided that such uses are permitted under federal and state law.

REFERENCES/CITATIONS

HITECH § 13405(b)

45 C.F.R. §§ 164.501, 164.506, 164.514(d)(3)(iii), 164.514(h) (2013)

65 Fed. Reg. 82462, 82489-91, 82498-99, 82500, 82524, 82537, 82538, 82545, 82546-47, 82600, 82632, 82682, 82686, 82715, 82718-20 (Dec. 28, 2000);

67 Fed. Reg. 53182, 53198, 53208-19 (Aug. 14, 2002)

78 Fed. Reg. 5660 (Jan. 25, 2013)

ARTICLE XIX - PERMITTED USES AND DISCLOSURES

SECTION E - RESEARCH

POLICY

Subject to the requirements of any BAAs and Participation Agreements with Participants, HIE shall obtain an individual's written authorization or satisfy an exception to the authorization requirement before using or disclosing the individual's PHI for research purposes. HIE employees whose responsibilities include using or disclosing PHI for research purposes shall be familiar with this Policy and shall follow the procedures set forth herein.

PROCEDURE

1. Determine That the Requested Use or Disclosure Is for Research Purposes. This Policy only applies when the purpose of the requested use or disclosure is research, defined as a systematic investigation including research development, testing, and evaluation that is designed to develop or contribute to generalizable knowledge. This Policy does not apply if the purpose of the requested use or disclosure is health care operations, defined to include quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination.

2. Determine That the Information To Be Used or Disclosed Is PHI. This Policy only applies if the information being used for research is PHI. If the information being used or disclosed has been completely de-identified, this Policy does not apply and HIE may use or disclose the de-identified information without following the procedures set forth in this Policy. De-identified data, meaning information that does not identify an individual and for which there is no reasonable basis to believe that the information can be used to identify an individual, which has been de-identified according to the methodology described in 45 C.F.R. § 164.514 is not subject to the Privacy Standards.

3. Obtain Individual Authorization or Satisfy an Exception to the Authorization Requirement. Once HIE has determined that the purpose of the requested use or disclosure is research and that the information to be used or disclosed is PHI, HIE shall obtain the written authorization of the individual who is the subject of the PHI **[or verify that Participant has obtained such written authorization]** or satisfy an exception to the authorization requirement before using or disclosing the individual's PHI for research purposes. Accordingly, to use or disclose PHI for research purposes, HIE must satisfy one of the following:

    a. *Obtain Written Authorization*. HIE may obtain the written authorization of each individual who is the subject of the PHI being used or disclosed for the research purposes, pursuant to Article XIX, Section F of these Model Privacy Policies.

b. *Obtain Representations From the Researcher That the Review Is Preparatory to Research*. HIE may rely on the following written representations from the researcher:

i. the use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;

ii. no PHI will be removed from HIE's premises by the researcher in the course of the review; and

iii. the PHI for which the use or access is sought is necessary for the research purposes.

HIE may *disclose* PHI in reliance on the above written representations only if the research project has been approved by an IRB.

HIE's use or disclosure of PHI under this paragraph 3(b) may enable a researcher to do the following: (i) review, but not remove, PHI to determine whether HIE has PHI relating to prospective research participants who may meet the eligibility criteria for enrollment in the researcher's study; or (ii) make a determination regarding whether there are a sufficient number of patients with a particular health condition within the community that would make the researcher's study feasible.

c. *Obtain Representations and Documentation From the Researcher That the Research Relates to Decedents' Information*. HIE may rely on the following from the researcher:

i. a representation that the use or disclosure is sought solely for research on the PHI of decedents;

ii. documentation, at the request of HIE, of the death of such individuals; and

iii. a representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

HIE may *disclose* PHI in reliance on the above only if the research project has been approved by an IRB.

d. *Obtain an IRB or Privacy Board Approval of the Waiver of or Alteration to the Otherwise Required Authorization*. HIE may rely on written documentation regarding the following:

i. The waiver of or alteration to the authorization has been approved by an IRB or a privacy board meeting specified standards;

ii. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

iii. The IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization, satisfies specified criteria;

iv. A brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board;

v. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and

vi. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or privacy board.

HIE may *disclose* PHI in reliance on the above documentation only if the research project has been approved by an IRB.

e. *Disclose a Limited Data Set Pursuant to a Data Use Agreement*. HIE is permitted to use or disclose a limited data set of information for research purposes pursuant to a Data Use Agreement without the prior written authorization of the individual(s) who is/are the subject of the information.

i. Limited Data Set. The information disclosed for the research purposes shall be limited to a limited data set. A limited data set excludes the following direct identifiers of the individuals or of relatives, employers, or household members of the individuals: (i) names; (ii) postal address information other than town or city, state, and zip code; (iii) telephone numbers; (iv) fax numbers; (v) e-mail addresses; (vi) Social Security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) Web Universal Resource Locators ("URLs"); (xiv) Internet Protocol ("IP") address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images. Identifiable information that may remain in the limited data set and therefore be disclosed for research purposes pursuant to this paragraph 3(e) includes dates relating to a patient (dates of service, admission, or discharge; date of birth; and date of death) and information relating to the town or city, state, and five-digit zip code of the patient, his or her employer, and the patient's household members.

ii. Data Use Agreement. Before HIE may use or disclose a limited data set of information for research purposes, HIE must enter into a Data Use Agreement with the recipient of the limited data set. The Data Use Agreement must: (i) establish the permitted uses and disclosures of the

information and may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the Privacy Standards or Security Standards if done by HIE; (ii) establish who is permitted to use or receive the limited data set; and (iii) provide that the limited data set recipient will: (a) not use or further disclose the information other than as permitted by the Data Use Agreement or as otherwise required by law; (b) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the Data Use Agreement; (c) report to HIE any use or disclosure of the information not provided for by its Data Use Agreement of which it becomes aware; (d) ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and (e) not identify the information or contact the individuals.

4. Make Minimum Necessary Uses and Disclosures. For purposes of paragraph 3(b) of this Policy, HIE is permitted to rely on the requesting researcher's representation that the purpose of the request is to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research and that the request meets the minimum necessary requirements unless an exception to the minimum necessary rules applies by law and pursuant to HIE's policies; HIE may only disclose to the requesting researcher the PHI specifically requested by the researcher. For purposes of paragraph 3(c) of this Policy, HIE is permitted to rely on the requesting researcher's representation that the purpose of the request is for research on the PHI of decedents and that the request meets the minimum necessary requirements; HIE may only disclose to the requesting researcher that PHI specifically requested by the researcher. For purposes of paragraph 3(d) of this Policy, HIE is permitted to rely on the statement in the IRB or Privacy Board Waiver or Alteration Form establishing the specific PHI for which use or access has been determined to be necessary by the IRB or privacy board; HIE shall only disclose the PHI specifically identified in the IRB or Privacy Board Waiver or Alteration Form.

5. Include Required Disclosures in the Accounting of Disclosures. Article VII of these Model Privacy Policies sets forth the procedures to be followed when an individual requests HIE to account for the disclosures of the individual's PHI. To the extent HIE discloses PHI for research purposes pursuant to an authorization in accordance with Article X, Section F of these Model Privacy Policies, or discloses a limited data set pursuant to a Data Use Agreement in accordance with paragraph 3(e) of this Policy, the disclosure(s) need not be included in the accounting. However, to the extent HIE discloses PHI for research purposes pursuant to an exception to authorization, the disclosure must be included in the accounting. .

6. Business Associate Agreements. HIE should review its BAAs with the applicable Participants and follow the terms of such agreements rather than this Policy, to the extent that such terms are more restrictive.

REFERENCES/CITATIONS

HITECH § 13405

45 C.F.R. §§ 164.508, 164.512(i) (2013)

65 Fed. Reg. 82462, 82520-21, 82536-38, 82543-45, 82575, 82625, 82656, 82689-90, 82694-99, 82701, 82702, 82710, 82740 (Dec. 28, 2000); 67 Fed. Reg. 14776, 14793-97 (Mar. 27, 2002); 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

OCR Guidance, pp. 96-97 (Dec. 3, 2002).

ARTICLE XIX- PERMITTED USES AND DISCLOSURES

SECTION F - MARKETING AND THE SALE OF PHI

POLICY

An authorization is generally required to use PHI for activities meeting the definition of Marketing in this Policy. In addition, PHI may not be disclosed in exchange for direct or indirect remuneration and, in the case of such remuneration, an authorization is generally required to use the PHI. HIE should consult with its own legal counsel prior to engaging in any Marketing. HIE's employees, whose responsibilities include Marketing shall be familiar with this Policy and shall follow these procedures.

TEXAS LAW ANALYSIS:

Under Section 181.153 of the Texas Health & Safety Code, as added by H.B. 300, a Texas Covered Entity, which is defined broadly enough to include HIE, may not disclose an individual's PHI in exchange for direct or indirect remuneration at all unless such disclosure is to another Texas Covered Entity or a "Covered Entity" as the term is defined in Section 602.001 of the Texas Insurance Code for the purpose of treatment, payment or health care operations or as otherwise authorized or required by state or federal law.

PROCEDURE

1. Definition.

Marketing. The term Marketing means:

i. to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

ii. Marketing does not include a communication made:

(1) to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for an individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonable related to the covered entity's cost of making the communication;

(2) for the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of individual by health care provider, including case management or care coordination for the individual, or to direct or recommend alternative

treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of the individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) In this context, financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual. .

2. No Disclosure of PHI in Exchange for Direct or Indirect Remuneration. HIE may not disclose PHI to any other person in exchange for financial remuneration except in very limited circumstances. HIE should consult with its own legal counsel prior to disclosing any PHI involving the exchange of remuneration.

3. Individual Authorization Generally Required for Use or Disclosure of PHI for Marketing. HIE must obtain an authorization prior to its use or disclosure of PHI for the purpose of Marketing, unless such communication falls within certain limited exceptions. Prior to making any such disclosures, HIE should consult with legal counsel and review the terms of its related BAAs and Participation Agreements.

REFERENCES/CITATIONS

HITECH § 13405

45 C.F.R. §§ 164, 164.508(a)(3); 164.501 (2013)

65 Fed. Reg. 82462, 82514, 82516, 82546, 82718, 82820 (Dec. 28, 2000); 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

67 Fed. Reg. 53,182; 53,185-90; 53,222-23 (Aug. 14, 2002)

78 Fed. Red. 5592-97 (Jan. 25, 2013)

TEX. HEALTH & SAFETY CODE ANN. §§ 181.001(b)(4)-(5), 181.152, as added and amended by HB 300.

TEX. HEALTH & SAFETY CODE § 241.153(8).

ARTICLE XIX - PERMITTED USES AND DISCLOSURES

SECTION G - LAW ENFORCEMENT, COURT ORDERS OR SUBPOENAS

POLICY

HIE may disclose PHI to a law enforcement official for a law enforcement purpose without patient authorization under the limited circumstances described in this policy. HIE employees whose responsibilities may include disclosing PHI to law enforcement officials shall be familiar with this Policy and shall follow these procedures.

PROCEDURE

1. Disclosures to Law Enforcement Officials for Law Enforcement Purposes. Subject to any more restrictive requirements which may be set forth in BAAs and/or Participation Agreements, PHI may be disclosed to a law enforcement official for a law enforcement purpose without prior written authorization under the circumstances described below. Disclosures that do not fall within an identified circumstance require prior written authorization in accordance with Article IV of these Model Privacy Policies. For purposes of this Policy, a law enforcement official is defined as an officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to: (1) investigate or conduct an official inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. The identity of a law enforcement official should be verified prior to disclosure of PHI.

    a. *Disclosures Permitted Pursuant to Process and as Otherwise Required by Law*. HIE may disclose PHI to a law enforcement official:

        i. To the extent required by law (meaning a mandate contained in law that compels a use or disclosure of PHI and is enforceable in a court of law), including laws that require the reporting of certain types of wounds or other physical injuries; or

        ii. In compliance with and as limited by the relevant requirements of:

            (1) A court order or court-ordered warrant;

            (2) A grand jury subpoena;

            (3) A subpoena or attachment issued by a judicial officer for a law enforcement purpose, in which the subject of the PHI is a party/defendant; or

            (4) An administrative request, including an administrative subpoena or summons, a civil or authorized investigative demand, or similar

process authorized under law, provided that (A) the information sought is relevant and material to a legitimate law enforcement inquiry; (B) the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; (C) the disclosure is to a federal, state or local government agency or authority; and (D) de-identified information could not reasonably be used. These conditions may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(5) A valid and complete subpoena or other official legal process issued at the request of an attorney (including "discovery requests") only if at least one of the following requirements is met. These requirements apply even if state law would otherwise allow such disclosure because the patient has put his or her condition or treatment at issue.

(A) The patient provides a written and dated Authorization to release the information to the requesting party.

(B) The subpoena or request is accompanied by a valid order from a court or administrative tribunal, as described above.

(C) Satisfactory assurance has been obtained from the party seeking the information that either (I) acceptable notice has been given to the patient, or (ii) an appropriate protective order has been obtained.

b. *Disclosures of Information About Victims or Suspected Victims of a Crime*. Except for disclosures required by law as permitted by paragraph 1(a) of this Policy, HIE may disclose PHI in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, if:

i. The individual orally agrees to the disclosure; or

ii. HIE is unable to obtain the individual's oral agreement because of incapacity or other emergency circumstance, provided that:

(1) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(2) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be

materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(3) The disclosure is in the best interests of the individual as determined by HIE, in the exercise of professional judgment.

c. *Disclosures of Information About a Decedent Whose Death Is Suspected to Have Resulted From Criminal Conduct*. HIE may disclose PHI of a decedent to a medical examiner or justice of the peace if the circumstances of the death require an inquest.

2. Individual Authorization Required for Other Disclosures of PHI. In order for HIE to disclose PHI to a law enforcement official for a law enforcement purpose without individual authorization, the disclosure must fall within one of the circumstances described in Paragraph 1 of this Policy. Disclosures that do not fall within an identified circumstance generally require prior written authorization in accordance with Article IV of these Model Privacy Policies.

REFERENCES/CITATIONS

45 C.F.R. §§ 164.512(f), 164.514(h)(2)(i)(A) 164.514(b) (2013).

65 Fed. Reg. 82462, 82531-34, 82672-73, 82678-87 (Dec. 28, 2000).

ARTICLE XIX- PERMITTED USES AND DISCLOSURES

SECTION H - PUBLIC AGENCY OVERSIGHT

POLICY

If and to the extent permitted by the terms of its BAAs and Participation Agreements, HIE may use and disclose PHI without prior written authorization for Health Oversight Activities authorized by law in accordance with the procedures described below. HIE workforce members who have the authority to use or disclose PHI for such purposes shall be familiar with this Policy and shall follow these procedures.

PROCEDURE

1. Health Oversight Activities. HIE may disclose PHI to a Health Oversight Agency for the following Health Oversight Activities that are authorized by law:

    a. audits;

    b. civil, administrative or criminal investigations (e.g., health care fraud investigations);

    c. inspections;

    d. licensure or disciplinary actions;

    e. civil, administrative or criminal proceedings or actions; or

    f. other activities necessary for appropriate oversight of the health care system (including oversight of health care plans; health benefit plans; health care providers; health care and health care delivery; resolution of consumer complaints; pharmaceuticals, medical products and devices, and dietary supplements; analysis of trends in health care costs, quality, health care delivery, access to care, and health insurance coverage); government benefit programs for which health information is relevant to beneficiary eligibility; entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or entities subject to civil rights laws for which health information is necessary for determining compliance.

2. Initiation of Disclosures Permitted. HIE may initial a disclosure of PHI for a health oversight activity; an investigation or proceeding does not have to be ongoing. For example, HIE can disclose PHI in the course of reporting suspected health care fraud to a health oversight agency, even if the agency has not yet conducted an investigation of HIE.

3. Verify Identity and Authority of Health Oversight Agency. Before disclosing PHI for a Health Oversight Activity, HIE shall verify the identity and authority of the Health Oversight Agency making the request as follows:

   a. HIE may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity:

      i. If the request is made in person, presentation of an agency identification badge, other official credentials or other proof of government status;

      ii. If the request is in writing, the request is on the appropriate government letterhead; or

      iii. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

   b. HIE may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

      i. A written statement of the legal authority under which the information is requested or, if a written statement would be impracticable, an oral statement of such authority; or

      ii. A warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, if the request is made pursuant to such legal process.

4. Disclose the Minimum Amount of PHI Necessary. HIE shall disclose only the minimum amount of PHI necessary to achieve the purpose of the disclosure unless an exception to minimum necessary applies by law and pursuant to HIE's policies. A minimum necessary disclosure for Health Oversight Activities could include large numbers of records to allow Health Oversight Agencies to perform, for example, statistical analysis to identify deviations in payment or billing patterns, as well as other data analyses.

5. Definition of "Health Oversight Agency." The term "Health Oversight Agency" means an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or

compliance, or to enforce civil rights laws for which health information is relevant. Health Oversight Agencies include, but are not limited to:

Texas Department of Insurance	Texas professional licensure agencies
Offices of Inspectors General	Department of Justice
Texas Health and Human Services Commission	Defense Criminal Investigative Services
Pension and Welfare Benefit Admin	HHS Office for Civil Rights
Food and Drug Admin.	Social Security Admin.
Department of Education	Occupational Health and Safety Admin.
Environmental Protection Agency	Equal Employment Opportunity Comm'n
Texas Department of Health	Drug Enforcement Admin.
Texas Department of Human Services	Medicare Carriers and Intermediaries

REFERENCES/CITATIONS

HITECH § 13405(b)(3)

45 C.F.R. §§ 164.501, 164.512(d) (2013)

65 Fed. Reg. 82462, 82476, 82491-92, 82528-29, 82530, 82544, 82547, 82610-11, 82671-74, 82719 (Dec. 28, 2000)

APPENDIX A

SAMPLE PARTICIPANT BUSINESS ASSOCIATE AGREEMENT

Instructions:

The Texas Health Services Authority (THSA) has developed a model BAA for use between providers (Covered Entities) and HIEs (Business Associates). The model BAA is **not required** for use by the HIEs. Rather, it was developed to provide a potential aid to reduce negotiating time between HIEs and providers. This model BAA is based on the BAA the Integrated Care Collaboration negotiated with its users. The main changes are the addition of some terms to address requirements under HB 300 (82nd Texas Legislature) and some changes to timeframes included in the document. The model BAA has also been amended to reflect the HIPAA/HITECH Omnibus Rule. This model BAA is not intended to serve as a substitute for legal advice, and HIEs that opt to use this document should consult an attorney to ensure that they use this document in such a way as to make it an enforceable BAA that meets applicable HIPAA and HITECH requirements.

Please note that Chapter 181 of the Texas Health and Safety Code defines the term "Covered Entity" more broadly than does HIPAA in 45 C.F.R. §160.103. The HIPAA definition, rather than the Texas definition, is used in this model BAA, as not all "covered entities" as defined by Texas law are required to comply with HIPAA and HITECH. However, all covered entities as defined by Chapter 181 are required to comply with the applicable Chapter 181 provisions.

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") dated _____, 2013 (the "Effective Date"), is entered into by and between _____ ("Covered Entity") and _____("Business Associate"), each a "Party" and collectively, the "Parties."

Covered Entity and Business Associate have entered into, are entering into, or may subsequently enter into, agreements or other documented arrangements (collectively, the "Business Arrangements") pursuant to which Business Associate may provide products and/or services for Covered Entity that require Business Associate to access, create, maintain, and use health information that is protected by state and/or federal law.

Pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the U.S. Department of Health & Human Services ("HHS") promulgated the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Standards"), at 45 C.F.R. Parts 160 and 164, requiring certain individuals and entities subject to the Privacy Standards (each a "Covered Entity", or collectively, "Covered Entities") to protect the privacy of certain individually identifiable health information ("Protected Health Information" or "PHI").

Pursuant to HIPAA, HHS issued the Security Standards (the "Security Standards"), at 45

C.F.R. Parts 160, 162 and 164, for the protection of electronic protected health information ("EPHI").

In order to protect the privacy and security of PHI, including EPHI, created or maintained by or on behalf of the Covered Entity, the Privacy Standards and Security Standards require a Covered Entity to enter into a "business associate agreement" with certain individuals and entities providing services for or on behalf of the Covered Entity if such services require the use or disclosure of PHI or EPHI.

On February 17, 2009, the federal Health Information Technology for Economic and Clinical Health Act was signed into law (the "HITECH Act"), and the HITECH Act imposes certain privacy and security obligations on Covered Entities in addition to the obligations created by the Privacy Standards and Security Standards.

The HITECH Act revises many of the requirements of the Privacy Standards and Security Standards concerning the confidentiality of PHI and EPHI, including extending certain HIPAA and HITECH Act requirements directly to Business Associates.

The HITECH Act requires that certain of its provisions be included in business associate agreements, and that certain requirements of the Privacy Standards be imposed contractually upon Covered Entities as well as Business Associates.

The Texas Legislature has adopted certain privacy and security requirements that are more restrictive than those required by HIPAA and HITECH, and such requirements are applicable to Business Associates as "Covered Entities" as defined by Texas law; and

Because Business Associate and Covered Entity desire to enter into this Business Associate Agreement, in consideration of the mutual promises set forth in this Agreement and the applicable Business Arrangements, and other good and valuable consideration, the sufficiency and receipt of which are hereby acknowledged, the Parties agree as follows:

1. Business Associate Obligations. Business Associate may receive from Covered Entity, or create or receive or maintain on behalf of Covered Entity, health information that is protected under applicable state and/or federal law, including without limitation, PHI and EPHI. All references to PHI herein shall be construed to include EPHI. Business Associate agrees not to use or disclose (or permit the use or disclosure of) PHI in a manner that would violate the Privacy Standards, Security Standards the HITECH Act, or Texas law, including without limitation the provisions of Texas Health and Safety Code Chapters 181 and 182 as amended by HB 300 (82nd Legislature), effective September 1, 2012, in each case including any implementing regulations as applicable (collectively referred to hereinafter as the "Confidentiality Requirements") if the PHI were used or disclosed by Covered Entity in the same manner.

2. Use of PHI. Except as otherwise required by law, Business Associate shall use PHI in compliance with 45 C.F.R. § 164.504(e). Furthermore, Business Associate shall use PHI (i)

solely for Covered Entity's benefit and only for the purpose of performing services for Covered Entity as such services are defined in Business Arrangements, (ii) for Data Aggregation Services (as hereinafter defined), and (iii) as necessary for the proper management and administration of the Business Associate or to carry out its legal responsibilities, provided that such uses are permitted under federal and state law. For avoidance of doubt, under no circumstances may Business Associate sell PHI in such a way as to violate Texas Health and Safety Code, Chapter 181.153, as amended by HB 300 (82nd Legislature), effective September 1, 2012, nor shall Business Associate use PHI for marketing purposes in such as manner as to violate Texas Health and Safety Code Section 181.152, or attempt to re-identify any information in violation of Texas Health and Safety Code Section 181.151, regardless of whether such action is on behalf of or permitted by the Covered Entity.

To the extent not otherwise prohibited in the Business Arrangements or by applicable law, use, creation and disclosure of de-identified health information, as that term is defined in 45 CFR § 164.514, by Business Associate is permitted.

3. Disclosure of PHI. Subject to any limitations in this Agreement, Business Associate may disclose PHI to any third party persons or entities as necessary to perform its obligations under the Business Arrangement and as permitted or required by applicable federal or state law. Business Associate recognizes that under the HIPAA/HITECH Omnibus Final Rule, Business Associates may not disclose PHI in a way that would be prohibited if Covered Entity made such a disclosure. Any disclosures made by Business Associate will comply with minimum necessary requirements under the Privacy Rule and related regulations.

3.1 Business Associate shall not [and shall provide that its directors, officers, employees, subcontractors, and agents, do not] disclose PHI to any other person (other than members of their respective workforce as specified in subsection 3.1(ii) below), unless disclosure is required by law or authorized by the person whose PHI is to be disclosed. Any such disclosure other than as specifically permitted in the immediately preceding sentences shall be made only if such disclosee has previously signed a written agreement that:

(i) Binds the disclosee to the provisions of this Agreement pertaining to PHI, for the express benefit of Covered Entity, Business Associate and, if disclosee is other than Business Associate, the disclosee;

(ii) Contains reasonable assurances from disclosee that the PHI will be held confidential as provided in this Agreement, and only disclosed as required by law for the purposes for which it was disclosed to disclosee; and

(iii) Obligates disclosee to immediately notify Business Associate of any breaches of the confidentiality of the PHI, to the extent disclosee has obtained knowledge of such breach.

3.2 Business Associate shall not disclose PHI to any member of its workforce and shall provide that its subcontractors and agents do not disclose PHI to any member of their respective workforces, unless Business Associate or such subcontractor or agent has advised such person of Business Associate's obligations

under this Agreement, and of the consequences for such person and for Business Associate or such subcontractor or agent of violating them as memorialized in a business associate agreement pursuant to the HIPAA/HITECH Omnibus Final Rule. Business Associate shall take and shall provide that each of its subcontractors and agents take appropriate disciplinary action against any member of its respective workforce who uses or discloses PHI in contravention of this Agreement.

3.3 In addition to Business Associate's obligations under Section 9, Business Associate agrees to mitigate, to the extent commercially practical, harmful effects that are known to Business Associate and is the result of a use or disclosure of PHI by Business Associate or Recipients in violation of this Agreement.

4. Access to and Amendment of Protected Health Information. Business Associate shall (i) provide access to, and permit inspection and copying of, PHI by Covered Entity; and (ii) amend PHI maintained by Business Associate as requested by Covered Entity. Any such amendments shall be made in such a way as to record the time and date of the change, if feasible, and in accordance with any subsequent requirements promulgated by the Texas Medical Board with respect to amendment of electronic medical records by HIEs. Business Associate shall respond to any request from Covered Entity for access by an individual within seven (7) days of such request and shall make any amendment requested by Covered Entity within twenty (20) days of the later of (a) such request by Covered Entity or (b) the date as of which Covered Entity has provided Business Associate with all information necessary to make such amendment. Business Associate may charge a reasonable fee based upon the Business Associate's labor costs in responding to a request for electronic information (or the fee approved by the Texas Medical Board for the production of non-electronic media copies). Business Associate shall notify Covered Entity within five (5) days of receipt of any request for access or amendment by an individual. Covered Entity shall determine whether to grant or deny any access or amendment requested by the individual. Business Associate shall have a process in place for requests for amendments and for appending such requests and statements in response to denials of such requests to the Designated Record Set, as requested by Covered Entity.

5. Accounting of Disclosures. Business Associate shall make available to Covered Entity in response to a request from an individual, information required for an accounting of disclosures of PHI with respect to the individual in accordance with 45 CFR § 164.528, as amended by Section 13405(c) of the HITECH Act and any related regulations or guidance issued by HHS in accordance with such provision.

6. Records and Audit. Business Associate shall make available to the United States Department of Health and Human Services or its agents, its internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by Business Associate on behalf of Covered Entity for the purpose of determining Covered Entity's compliance with the Confidentiality Requirements or the requirements of any other health oversight agency, in a time and manner designated by the Secretary.

7. Implementation of Security Standards; Notice of Security Incidents. Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as expressly permitted under this Agreement. Business Associate will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate acknowledges that the HITECH Act requires Business Associate to comply with 45 C.F.R. §§164.308, 164.310, 164.312 and 164.316 as if Business Associate were a Covered Entity, and Business Associate agrees to comply with these provisions of the Security Standards and all additional security provisions of the HITECH Act.

Furthermore, to the extent feasible, Business Associate will use commercially reasonable efforts to secure PHI through technology safeguards that render such PHI unusable, unreadable and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI in accordance with HHS Guidance published at 74 Federal Register 19006 (April 17, 2009), or such later regulations or guidance promulgated by HHS or issued by the National Institute for Standards and Technology ("NIST") concerning the protection of identifiable data such as PHI. Lastly, Business Associate will promptly report to Covered Entity any successful Security Incident of which it becomes aware. At the request of Covered Entity, Business Associate shall identify: the date of the Security Incident, the scope of the Security Incident, the Business Associate's response to the Security Incident and the identification of the party responsible for causing the Security Incident, if known.

8. Data Breach Notification and Mitigation.

8.1 HIPAA Data Breach Notification and Mitigation. Business Associate agrees to implement reasonable systems for the discovery and prompt reporting to Covered Entity of any "breach" of "unsecured PHI" as those terms are defined by 45 C.F.R. § 164.402. Specifically, a breach is an unauthorized acquisition, access, use or disclosure of unsecured PHI, including ePHI, which compromises the security or privacy of the PHI/ePHI. A breach is presumed to have occurred unless there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed in 45 C.F.R. § 164.402(2)(i)-(iv) (hereinafter a "HIPAA Breach"). The parties acknowledge and agree that 45 C.F.R. § 164.404, as described below in this Section 8.1, governs the determination of the date of discovery of a HIPAA Breach. In addition to the foregoing and notwithstanding anything to the contrary herein, Business Associate will also comply with applicable state law, including without limitation, Section 521 Texas Business and Commerce Code, as amended by HB 300 (82nd Legislature), or such other laws or regulations as may later be amended or adopted. In the event of any conflict between this Section 8.1, the Confidentiality Requirements, Section 521 of the Texas Business and Commerce Code, and any other later amended or adopted laws or regulations, the most stringent requirements shall govern.

8.2 Discovery of Breach. Business Associate will, following the discovery of a HIPAA Breach, notify Covered Entity without unreasonable delay and in no event later than the earlier of the maximum of time allowable under

applicable law or three (3) business days after Business Associate discovers such HIPAA Breach, unless Business Associate is prevented from doing so by 45 C.F.R. §164.412 concerning law enforcement investigations. For purposes of reporting a HIPAA Breach to Covered Entity, the discovery of a HIPAA Breach shall occur as of the first day on which such HIPAA Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. Business Associate will be considered to have had knowledge of a HIPAA Breach if the HIPAA Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the HIPAA Breach) who is an employee, officer or other agent of the Business Associate.

8.3 Reporting a Breach. Without unreasonable delay and no later than the earlier of the maximum of time allowable under applicable law or five (5) business days following a HIPAA Breach, Business Associate shall provide Covered Entity with sufficient information to permit Covered Entity to comply with the HIPAA Breach notification requirements set forth at 45 C.F.R. § 164.400 *et seq.* Specifically, if the following information is known to (or can be reasonably obtained by) the Business Associate, Business Associate will provide Covered Entity with:

(i) contact information for individuals who were or who may have been impacted by the HIPAA Breach (e.g., first and last name, mailing address, street address, phone number, email address);

(ii) a brief description of the circumstances of the HIPAA Breach, including the date of the HIPAA Breach and date of discovery;

(iii) a description of the types of unsecured PHI involved in the HIPAA Breach (e.g., names, social security number, date of birth, addressees, account numbers of any type, disability codes, diagnostic and/or billing codes and similar information);

(iv) a brief description of what the Business Associate has done or is doing to investigate the HIPAA Breach, mitigate harm to the individual impacted by the HIPAA Breach, and protect against future HIPAA Breaches; and

(v) appoint a liaison and provide contact information for same so that Covered Entity may ask questions or learn additional information concerning the HIPAA Breach.

Following a HIPAA Breach, Business Associate will have a continuing duty to inform Covered Entity of new information learned by Business Associate regarding the HIPAA Breach, including but not limited to the information described in items (i) through (v), above.

9. Termination.

9.1 This Agreement shall commence on the Effective Date.

9.2 Upon the termination of the applicable Business Arrangement, either Party may terminate this Agreement by providing written notice to the other Party.

9.3 Upon termination of this Agreement for any reason, Business Associate agrees:

(i) to return to Covered Entity or to destroy all PHI received from Covered Entity or otherwise through the performance of services for Covered Entity, that is in the possession or control of Business Associate or its agents. Business Associate agrees that all paper, film, or other hard copy media shall be shredded or destroyed such that it may not be reconstructed, and EPHI shall be purged or destroyed concurrent with NIST Guidelines for media sanitization at http://www.csrc.nist.gov/; or

(ii) in the case of PHI which is not feasible to "return or destroy," to extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. Business Associate further agrees to comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatment of such PHI.

10. Miscellaneous.

10.1 Notice. All notices, requests, demands and other communications required or permitted to be given or made under this Agreement shall be in writing, shall be effective upon receipt or attempted delivery, and shall be sent by (i) personal delivery; (ii) certified or registered United States mail, return receipt requested; (iii) overnight delivery service with proof of delivery; or (iv) facsimile with return facsimile acknowledging receipt. Notices shall be sent to the addresses below. Neither party shall refuse delivery of any notice hereunder.

Covered Entity:

_____
_____
_____
_____

Business Associate:

_____
_____
_____
_____

10.2 Waiver. No provision of this Agreement or any breach thereof shall be deemed waived unless such waiver is in writing and signed by the Party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.

10.3 Assignment**.** Neither Party may assign (whether by operation or law or otherwise) any of its rights or delegate or subcontract any of its obligations under this Agreement without the prior written consent of the other Party. Notwithstanding the foregoing, Covered Entity shall have the right to assign its rights and obligations hereunder to any entity that is an affiliate or successor of Covered Entity, without the prior approval of Business Associate.

10.4 Severability. Any provision of this Agreement that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

10.5 Entire Agreement. This Agreement constitutes the complete agreement between Business Associate and Covered Entity relating to the matters specified in this Agreement, and supersedes all prior representations or agreements, whether oral or written, with respect to such matters. In the event of any conflict between the terms of this Agreement and the terms of the Business Arrangements or any such later agreement(s), the terms of this Agreement shall control unless the terms of such Business Arrangements are more strict with respect to PHI and comply with the Confidentiality Requirements, or the parties specifically otherwise agree in writing. No oral modification or waiver of any of the provisions of this Agreement shall be binding on either Party; provided, however, that upon the enactment of any law, regulation, court decision or relevant government publication and/or interpretive guidance or policy that the Covered Entity believes in good faith will adversely impact the use or disclosure of PHI under this Agreement, Covered Entity may amend the Agreement to comply with such law, regulation, court decision or government publication, guidance or policy by delivering a written amendment to Business Associate which shall be effective thirty (30) days after receipt. No obligation on either Party to enter into any transaction is to be implied from the execution or delivery of this Agreement. This Agreement is for the benefit of, and shall be binding upon the parties, their affiliates and respective successors and assigns. No third party shall be considered a third-party beneficiary under this Agreement, nor shall any third party have any rights as a result of this Agreement.

10.6 Governing Law. This Agreement shall be governed by and interpreted in accordance with the laws of the state of Texas. Venue for any dispute relating to this Agreement shall be in Travis County, Texas.

10.7 Nature of Agreement; Independent Contractor. Nothing in this Agreement shall be construed to create (i) a partnership, joint venture or other joint business relationship between the parties or any of their affiliates, or (ii) a

relationship of employer and employee between the parties. Business Associate is an independent contractor, and not an agent of Covered Entity. This Agreement does not express or imply any commitment to purchase or sell goods or services.

10.8 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same document. In making proof of this Agreement, it shall not be necessary to produce or account for more than one such counterpart executed by the party against whom enforcement of this Agreement is sought. Signatures to this Agreement transmitted by facsimile transmission, by electronic mail in portable document format (".pdf") form, or by any other electronic means intended to preserve the original graphic and pictorial appearance of a document, will have the same force and effect as physical execution and delivery of the paper document bearing the original signature.

10.9 Definitions. For the purposes of this Agreement, the following definitions shall apply:

(i) *"Business Associate"* shall have the meaning given to the term "Associate" under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

(ii) *"Covered Entity"* shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR Section 160.103.

(iii) "*Data Aggregation Services*" shall mean the combining of PHI or EPHI by Business Associate with the PHI or EPHI received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of, payment to, and treatment of patients by the respective covered entities.

(iv) *"Electronic Protected Health Information"* or *"EPHI"* shall have the meaning given to such term under the HIPAA Rule, including but not limited to 45 CFR Parts 160, 162, and 164, and under HITECH.

(v) *"Privacy Rule"* shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160, 162 and 164.

(vi) *"Security Rule"* shall mean the HIPAA regulation that is codified at 45 C.F.R. Part 164.

(vii) *"Protected Health Information"* or *"PHI"* means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule,

including, but not limited to, 45 CFR Section 164.501. *[45 CFR §§160.103 and 164.501.*

(viii) The Health Information Technology for Economic and Clinical Health ("HITECH") Act shall mean Division A, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5). The U.S. Department of Health and Human Services ("HHS") omnibus final rule at 78 Fed. Reg. 5555-5702 implements the privacy, security, enforcement, and breach notice provisions of HITECH.

(ix) Any other capitalized term not otherwise defined in this Section 13.10 or this Agreement shall have the meanings set forth in the Privacy Standards, Security Standards or the HITECH Act, as applicable.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
_____	_____
By:_____	By_____
Title:_____	Title:_____
Date:_____	Date:_____

APPENDIX B

SAMPLE WORKFORCE TRAINING LOG

Name:

Position:

Date of Initial Privacy Training:

Date of Additional Privacy Training:

Date Health Information Confidentiality Agreement Signed:

Date Provided Access to Protected Health Information:

Date Access to Protected Health Information Terminated:

Sanctions and Disciplinary Action:

APPENDIX C

WORKFORCE MEMBER
HEALTH INFORMATION CONFIDENTIALITY AGREEMENT

This Health Information Confidentiality Agreement ("Agreement") applies to all members of HIE's workforce including staff, employees, volunteers, independent contractors, trainees and others who, in the performance of work for HIE, are under HIE's direct control and who have access to protected health information ("PHI") maintained, received, or transmitted by HIE.

Please read all sections of this Agreement, in addition to HIE's privacy and security policies and procedures, before signing below.

HIE has a legal and ethical responsibility to safeguard the privacy and protect the confidentiality of PHI it may receive, store, aggregate or transmit. In the course of your employment, you may hear information that relates to an individual's health, read or see computer or paper files containing PHI and/or create documents containing PHI. Because you may have contact with PHI, HIE requests that you agree to the following as a condition of your employment:

1. Confidential PHI.

   I understand that all health information that may in any way identify a patient or relate to a patient's health must be maintained confidentially. I will regard confidentiality as a central obligation of my job responsibilities.

2. Prohibited Use and Disclosure.

   I agree that, except as required under my job responsibilities or as directed by HIE, I will not at any time during or after my work for HIE speak about or share any PHI with any person or permit any person to examine or make copies of any PHI maintained by HIE. I understand and agree that personnel who have access to health records must preserve the confidentiality and integrity of such records, and no one is permitted access to the health record of any patient without a necessary, legitimate, work-related reason. I shall not, nor shall I permit any person to, inappropriately examine or photocopy a patient record or remove a patient record from HIE.

3. Safeguards.

   When PHI must be discussed with other healthcare practitioners in the course of my work for HIE, I shall make reasonable efforts to avoid such conversations from being overheard by others who are not involved in the patient's care.

   I understand that when PHI is within my control, I must use all reasonable means to prevent it from being disclosed to others, except as otherwise permitted by this

Agreement. I will not at any time reveal to anyone my confidential access codes to HIE's information systems, and I will take all reasonable measures to prevent the disclosure of my access codes to anyone. I also understand that HIE may, at any time, monitor and audit my use of the electronic/automated patient record and information systems.

Protecting the confidentiality of PHI means protecting it from unauthorized use or disclosure in any form: oral, fax, written, or electronic. If I keep patient notes on a handheld or laptop computer or other electronic device, I will ensure that my supervisor knows of and has approved such use. I agree not to send patient identifiable health information in an email, or email attachment, unless I am directed to do so by my supervisor.

4. Training and Policies and Procedures.

I certify that I have read HIE's policies and procedures, completed the training courses offered by HIE, and shall abide by HIE's policies and procedures governing the protection of PHI.

5. Return or Destruction of Health Information.

If, as part of my job responsibilities, I must take PHI off the premises of HIE, I shall ensure that I have HIE's permission to do so, I shall protect the PHI from disclosure to others, and I shall ensure that all of the PHI, in any form, is returned to HIE or destroyed in a manner that renders it unreadable and unusable by anyone else.

6. Termination.

At the end of my employment with HIE, or when my assignment for HIE is otherwise terminated, I will make sure that I take no PHI with me, and that all PHI in any form is returned to HIE or destroyed in a manner that renders it unreadable and unusable by anyone else. Discharge or termination, whether voluntary or not, shall not affect my ongoing obligation to safeguard the confidentiality of PHI and to return or destroy any such PHI in my possession.

7. Sanctions.

I understand that my unauthorized access or disclosure of PHI may violate state or federal law and cause irreparable injury to HIE and harm to the patient who is the subject of the PHI and may result in disciplinary and/or legal action being taken against me, including termination of my employment.

8. Reporting of Non-Permitted Use.

I agree to immediately report to HIE any unauthorized use or disclosure of PHI by any person. The person to whom I report unauthorized uses and disclosures is **[title of person or position at telephone number XXX-XXX-XXXX]**.

9. Disclosure to Third Parties.

I understand that I am not authorized to share or disclose any PHI with or to anyone who is not part of HIE's workforce, unless otherwise permitted by this Agreement.

10. Agents of the Department of Health and Human Services.

I agree to cooperate with any investigation by the Secretary of the U.S. Department of Health and Human Services ("HHS"), or any agent or employee of HHS or other oversight agency, for the purpose of determining whether HIE is in compliance federal or state privacy laws.

11. Disclosures Required by Law.

I understand that nothing in this Agreement prevents me from using or disclosing PHI if I am required by law to use or disclose PHI.

By my signature below, I agree to abide by all the terms and conditions of this Agreement.

Signature of Workforce Member: _____

Printed Name: _____

Date: _____

Address: _____

_____

Phone: _____

APPENDIX D

CONCERNS OR COMPLAINTS REGARDING PRIVACY PRACTICES

[Logo]
Concerns or Complaints Regarding Privacy Practices

HIE takes its privacy responsibilities very seriously. To help us make sure that your concerns are properly addressed, please take the time to fill out this form in as much detail as possible.

Your name: _____ Date: _____
Address: _____ Daytime phone number: _____
_____

If this involves a particular patient or event, please give the following:

Patient's name: _____ Phone number: _____

Names (if known) or description of persons involved: _____
_____
_____
_____

Date, time, and place of occurrence: _____

Describe the event and your concerns in as much detail as possible:
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

(If necessary, continue on reverse side of page)

_ _

For HIE Use Only:

Date received: _____
Received by: _____
Date forwarded to Privacy Officer: _____

Investigation and Resolution of Complaint

Date of Complaint: _____ Patient: _____
Person who complained (if different): _____
Telephone number: _____

Summary of concern or complaint:
_____
_____
_____
_____

Describe steps taken to investigate:
_____
_____
_____
_____
_____

Date investigation completed: _____

Was complaint found to be justified? Explain why or why not:
_____
_____
_____
_____

Recommended actions:
_____
_____
_____
_____
_____

Date of contact with person who complained: _____

Contacted by: _____ (attach letter if person contacted in writing)

Did the person express further concerns? If so, describe:
_____
_____
_____

This page is left intentionally blank.