Attachments Document

THSA Board Meeting

November 1, 2019

Attachment No. 1

Amendments to HIETexas Privacy & Security Policies & Procedures

TEXAS HEALTH SERVICES AUTHORITY
HEALTH INFORMATION POLICY
REGARDING PRIVACY OF HEALTH INFORMATION

TABLE OF CONTENTS

PAGE

ARTICLE I - INTRODUCTION

Introduction			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: ~~*September 23, 2013*~~*May 12, 2019*	Board of Directors Approval: ~~*September 27, 2013*~~*November 1, 2019*	Article: *I*	Version: *1.*~~*0*~~*1*

The Texas Health Services Authority (THSA) Health Information Policy Regarding Privacy ~~and Security~~ of Protected Health Information (PHI) is hereby adopted and approved by THSA, and it shall be effective as of the Effective Date. Where and when appropriate, these policies and procedures shall apply the protections and safeguards for Texas HHS Confidential Information in the same manner as they do for PHI. The Policy is comprised of two separate sets of policies: a set of Privacy Policies and a set of Security Policies. This document contains the ~~Security~~ Privacy Policies; the ~~Privacy~~ Security Policies are contained in an accompanying document.

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

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

~~In 2010, the Department of Health and Human Services, through the Office of the National Coordinator for Health Information Technology, approved Texas's Strategic and Operational Plan for Statewide HIE, under which the state received grant funding to further certain health information exchange goals. As part of this program, which is being administered by the Texas Health and Human Services Commission (HHSC) with contractual support from the THSA, the HHSC helped to fund 12 regional HIE networks, the Local HIEs, which cover approximately 90% of the state's physicians and hospitals eligible for the program.~~

~~**Business Associates and HIPAA/HITECH Compliance**. The HITECH Act extended the security requirements of HIPAA to Business Associates of Covered Entities. In the HIPAA Omnibus Rule, the Office for Civil Rights specified that a health information organization, or HIE (such as the THSA), is a Business Associate under HIPAA.[2] Therefore, HIEs must comply with~~

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

~~[2] *See* 45 C.F.R. §§ 160.103.~~

~~the elements of the Privacy and Security Rules that apply to Business Associates under HIPAA and HITECH.~~

~~While the THSA is specifically designated as a business associate under HIPAA, members of the THSA workforce do not receive or access protected health information (PHI). The THSA instead delegates this responsibility to its technology subcontractor, InterSystems Corporation, which is also considered a business associate under HIPAA. Regardless of whether THSA workforce members have access to PHI, the THSA adopts these Privacy policies to account for any unforeseen situation in which a THSA workforce member may access PHI.~~

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

ARTICLE II - DEFINITIONS

Definitions			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: ~~*September 23, 2013*~~*May 12, 2019*	Board of Directors Approval: ~~*September 27, 2013*~~*November 1, 2019*	Article: *II*	Version: *1.*~~*0*~~*1*

Unless otherwise ~~provided~~defined in these Privacy Policies, the following ~~definitions in this Article II shall be used in the interpretation of these Privacy Policies~~terms shall adopt the definitions contained in the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act (HIPAA):

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.

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 - September 23, 2013~~

~~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.

HHS DUA – Texas Health and Human Services Data Use Agreement; the agreement that HHSC requires covered entities to sign before exchanging data or entering into such a contract with HHSC.

HIE – Means health information exchange.~~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~~The statewide health information exchange for the State of Texas, which is operated by THSA under Chapter 182, Texas Health & Safety Code.

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.

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).

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.~~

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

Participant - an individual or entity that accesses, receives or transmits PHI to or through HIETexas, and enters into a Participation Agreement with the THSA.

Participation Agreement - Agreement between the THSA 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 ~~–~~ Means Texas Health Services Authority created by Chapter 182 of the Texas Health and Safety Code.

TPO - treatment, payment, and healthcare operations.

Workforce – Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the THSA, is under the direct control of the THSA, whether or not they are paid by the THSA.

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 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 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

Privacy Officer			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: *~~September 23, 2013~~May 12, 2019*	Board of Directors Approval: *~~September 27, 2013~~November 1, 2019*	Article: *III*	Version: *1.~~0~~1*

POLICY

The THSA 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. The THSA should regularly update and maintain its documentation of privacy personnel designations, where applicable.

The THSA has not appointed a Privacy Officer at this time, but will follow the below-listed procedures if one is appointed at a future date.

PROCEDURE

1. Privacy Officer. The THSA may appoint a Privacy Officer to (i) report directly to its Chief Executive Officer, (ii) also to report directly to the board of directors, and (iii) work with its Security Officer and/or General Counsel to ensure compliance with the Privacy Standards or Security Standards. The Privacy Officer may be contacted at privacy@thsa.org.

2. Qualifications. The THSA may maintain certain qualifications of its Privacy Officer. The following is a non-exhaustive list of potential Privacy Officer qualifications that the THSA 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;

    ~~e.~~f. possession of industry certifications, including but not limited to CHPC, CIPP/US, CIPM, and/or CIPT; and

~~f.~~g. 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. The THSA 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 the THSA's staff to establish an organization-wide interdisciplinary Privacy & Security 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 Privacy & Security task force referenced in Paragraph 3(a).

c. Designate a Contact Person (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 Privacy & Security 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 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 that the THSA 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 the THSA's privacy policies and procedures in coordination with management and administration, the Privacy & Security task force, and legal counsel.

h. Ensure that the privacy policies and procedures are regularly reviewed and updated in line with state and federal requirements, as well as the requirements of the Texas HHS DUA.

i. Prepare a report on a periodic basis for the Board, CEO, and Privacy and Security 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 the THSA (and its related entities).

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

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

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

p. Initiate and conduct an internal privacy audit program.

q. Establish, with the THSA's management, operations, and Security Officer, a mechanism to track access to PHI within the THSA'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 THSA 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 the THSA's Security Officer and/or General Counsel to establish a process for receiving, documenting, tracking, investigating, and taking corrective action on all complaints concerning the THSA'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 the THSA's workforce, extended workforce, and for all Business Associates, in cooperation with Security Officer and/or General 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 the THSA's privacy policies and procedures and applicable federal and state laws and regulations.

y. Cooperate with HHS, OCR, other legal entities, as well as, THSA 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 the THSA's workforce members receiving privacy training on time and according to mandated schedules;

    vi. percentage of the THSA'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, the THSA's Privacy and Security Task Force (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 the THSA'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

Consent or Authorization			
Texas Health Services Authority	**Privacy Policies & Procedures**		
Effective Date: *September 23, 2013*	Board of Directors Approval: *September 27, 2013*	Article: *IV*	Version: *1.0*

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 (including subcontractors), such as the THSA, may use or disclose PHI only as allowed under its Business Associate Agreement with the relevant Business Associate or 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 THSA and the Business Associate or Covered Entity must be passed down in the related Business Associate Agreement should the THSA engage a subcontractor.

Under the Texas Medical Records Privacy Act, the THSA 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 the THSA or its Participant.

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

However, many Covered Entities and Business Associates do elect 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 Covered Entities and Business Associate may require consent or authorization for uses and disclosures of PHI for treatment, payment and health care operations when not Required by Law. Other Covered Entities and Business Associate 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.

The THSA should work with its Participants and legal counsel of their Participants to carefully identify what types of information will be used or disclosed by the THSA, 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. The THSA may want to include in its 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, the THSA 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

Patient Preference			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: *September 23, 2013*	Board of Directors Approval: *September 27, 2013*	Article: *V*	Version: *1.0*

POLICY

The THSA will adhere to the consent policies of each of its Participants, who 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

Because patient preference is addressed at the provider or HIE level, the THSA shall redirect any requests regarding patient preference to the applicable Participant. The THSA shall maintain a log of all requests received from an individual regarding patient preference. The THSA shall make this log available to all Participants for review.

If the THSA receives a request from an individual regarding patient preference, and the individual has provided sufficient contact information regarding the individual's address, the THSA shall notify the applicable Participant within five (5) business days. If the individual fails to provide sufficient contact information to the THSA regarding the individual's address, then the THSA shall make a good-faith effort to obtain the individual's address so that the THSA may properly redirect the individual's request to the proper HIETexas Participant.

The Participant will address the requests in accordance with the Participant's policy on patient preference. The Participant will notify the THSA within five (5) business days after the Participant's resolution of the individual's request. If the Participant fails to notify the THSA within five (5) business days after the Participant's resolution of the individual's request, then the THSA shall make a good-faith effort to determine if the request has been resolved.

ARTICLE VI - NOTICE OF DATA PRACTICES, ELECTRONIC DISCLOSURE

Notice of Data Practices, Electronic Disclosure			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: *September 23, 2013*	Board of Directors Approval: *September 27, 2013*	Article: *VI*	Version: *1.0*

POLICY

While the THSA's primary purpose is to facilitate the transmission of health data, in order to comply with State Law in the THSA's capacity as a Texas Covered Entity, the THSA shall provide written notice to patients for whom it creates or receives PHI if the PHI is subject to electronic disclosure. The written notice will be posted. THSA employees who are responsible for posting this notice 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 THSA, 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 HIETexas.

PROCEDURE

Post Written Notice of Possible Electronic Disclosure of PHI. The THSA shall provide general notice to patients that their PHI is subject to electronic disclosure.

Provide Language to Include in Participants' Notice of Privacy Practices. The THSA and its Participants may deem it beneficial for the THSA to develop language that can or must be included in Participants' Notices of Privacy Practices regarding transfer or exchange of PHI to or by the THSA. To the extent that such privacy practices may change over time, the THSA and its Participants may want to ensure that Participants retain 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

Accounting of Who Has Accessed PHI and to whom PHI has been Disclosed			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: *~~September 23, 2013~~May 12, 2019*	Board of Directors Approval: *~~September 27, 2013~~November 1, 2019*	Article: *VII*	Version: *1.~~0~~1*

POLICY

The THSA recognizes an individual's right to receive an accounting ("accounting") of certain disclosures of an access to the individual's PHI made through HIETexas in the six years prior to the date on which the accounting is requested. THSA employees whose responsibilities include receiving requests for accountings and processing and providing accountings shall be familiar with this Policy and shall follow these procedures. The THSA 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. The THSA hereby designates the ~~following~~ THSA Privacy Officer as the ~~person~~ role responsible for receiving and processing requests for an accounting:

   ~~**Anne Kimbol**~~**THSA Privacy Officer**
   ~~General Counsel~~
   Texas Health Services Authority
   ~~221 E. 9th Street, Ste. 201~~901 S. Mopac Expressway, Building 1, Ste. 300
   Austin, Texas ~~78701~~78746
   (512) ~~814-0321 (ext. 303)~~329-2730
   Privacy@thsa.org ~~Anne.Kimbol@thsa.org~~

2. Recognize an Individual's Right to Request an Accounting. The THSA shall recognize an individual's right to receive an accounting of certain disclosures of the individual's PHI made through HIETexas and/or of who has access the individual's PHI through HIETexas in the six years prior to the date on which the accounting is requested. If the THSA receives a request for an accounting from an individual relating to such individual's PHI that has not been made by the THSA but has instead been made by a Participant through HIETexas, the THSA 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. The THSA 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 the THSA's subcontractors unless the disclosure is excepted from the accounting requirements. If an individual requests an accounting, the THSA will contact its subcontractors to whom the THSA 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 the THSA 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, or 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 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, the THSA 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, the THSA may provide the accounting to the Participant to forward to the individual or provide the accounting directly to the individual. The THSA 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. The THSA 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. The THSA 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, AMENDMENT, AND COPYING OF PHI

Access, Amendment, and Copying of PHI			
Texas Health Services Authority	**Privacy Policies & Procedures**		
Effective Date: *September 23, 2013*	Board of Directors Approval: *September 27, 2013*	Article: *VIII*	Version: *1.0*

POLICY

The THSA 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 the THSA does not maintain PHI in a "designated record set," as defined by HIPAA, the THSA shall make all reasonable efforts to redirect the individual to the proper Participant to fulfill the individual's request. In the case of a request from an individual, the THSA's BAA and/or Participation Agreement will dictate whether the THSA provides this information to an individual or forwards the request to the Participant, which shall manage the process. THSA employees who receive patient requests to inspect and copy records shall be familiar with this policy and shall follow these procedures.

PROCEDURE

The THSA shall maintain a log of all requests received from an individual to access, copy, and/or amend his or her PHI. The THSA shall make this log available to its Participants for review.

If the THSA receives a request from an individual to access, copy, and/or amend his or her PHI, and the individual has provided sufficient contact information regarding the individual's address, the THSA shall notify the applicable Participant within five (5) business days. If the individual fails to provide sufficient contact information to the THSA regarding the individual's address, then the THSA shall make a good-faith effort to obtain the individual's address so that the THSA may properly redirect the individual's request to the proper HIETexas Participant.

The Participant will address the requests in accordance with the Participant's policy on accessing, copying, and/or amending an individual's PHI. The Participant will notify the THSA within five (5) business days after the Participant's resolution of the individual's request. If the Participant fails to notify the THSA within five (5) business days after the Participant's resolution of the individual's request, then the THSA shall make a good-faith effort to determine if the request has been resolved.

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.

ARTICLE IX - REQUEST FOR RESTRICTIONS

Request for Restrictions			
Texas Health Services Authority	**Privacy Policies & Procedures**		
Effective Date: *September 23, 2013*	Board of Directors Approval: *September 27, 2013*	Article: *IX*	Version: *1.0*

POLICY

The THSA 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 the THSA 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 THSA of any restrictions and require the THSA, as a Business Associate, to honor such restrictions. THSA employees who have the authority to disclose PHI shall be familiar with this Policy and shall follow these Procedures.

PROCEDURE

The THSA shall maintain a log of all requests received from an individual regarding a request for restrictions of PHI. The THSA shall make this log available to its Participants for review.

If the THSA receives a request from an individual regarding requests for restrictions of PHI, and the individual has provided sufficient contact information regarding the individual's address, the THSA shall notify the applicable Participant within five (5) business days. If the individual fails to provide sufficient contact information to the THSA regarding the individual's address, then the THSA shall make a good-faith effort to obtain the individual's address so that the THSA may properly redirect the individual's request to the proper HIETexas Participant.

The Participant will address the requests in accordance with the Participant's policy regarding requests for restrictions of PHI. The Participant will notify the THSA within five (5) business days after the Participant's resolution of the individual's request. If the Participant fails to notify the THSA within five (5) business days after the Participant's resolution of the individual's request, then the THSA shall make a good-faith effort to determine if the request has been resolved.

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 X - ROLE-BASED WORKFORCE TRAINING

Role-Based Workforce Training			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: *September 23, 2013*	Board of Directors Approval: *September 27, 2013*	Article: *X*	Version: *1.0*

POLICY

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

PROCEDURE

1. Training Required. This policy shall act as the THSA's policy requiring its individual workforce members to attend scheduled training conducted or provided by the THSA. The THSA may institute 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. Training Content. The training received by a workforce member will be necessary and appropriate for the workforce member to carry out his or her duties for the THSA.

3. Responsibility for Training. The THSA 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 form of training is necessary and appropriate for the workforce member to carry out his or her duties for the THSA through role-playing, case studies, seminars and discussions, in addition to traditional lectures, video presentations or interactive software programs;

f. maintaining all documentation of training for a period of six years; and

g. developing competency tests to evaluate training effectiveness.

4. Initial Training. The THSA 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 the THSA'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. In the event of a material change in the THSA'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 not later than one year after the material change becomes effective.

6. Documentation. The THSA 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 6 years from the date of their creation. Further, the THSA 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. The THSA shall maintain the signed statement for its records for a period of six years. The THSA will place 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 may 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 the THSA'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 H.B. 300 (82R), and amended by S.B. 1609 (83R).

ARTICLE XI - RECEIVING AND RESOLVING COMPLAINTS

Receiving and Resolving Complaints			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: ~~*September 23, 2013*~~*May 12, 2019*	Board of Directors Approval: ~~*September 27, 2013*~~*November 1, 2019*	Article: *XI*	Version: *1.~~0~~1*

POLICY

The THSA may have a process by which any person can make a complaint to the THSA or the Secretary regarding the THSA's privacy policies, procedures, and/or practices, as well as, the THSA's compliance with its privacy policies and procedures and the Privacy Standards and Security Standards. However, if the THSA develops a process for complaints to the Secretary, then that process will be consistent with 45 C.F.R. § 160.306. The THSA 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.

PROCEDURE

1. Designation of Contact Person. The THSA may allow the designation of a Contact Person for all complaints. The Contact Person shall 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. The following person shall act as the contact person to receive the above-listed complaints:

   ~~**Anne Kimbol**~~**THSA Privacy Officer**
   ~~General Counsel~~
   Texas Health Services Authority
   ~~221 E. 9th Street, Ste. 201~~901 S. Mopac Expressway, Building 1, Ste. 300
   Austin, Texas ~~78701~~78746
   ~~(512) 814-0321 (ext. 303)~~512-329-2730
   ~~Anne.Kimbol@thsa.org~~Privacy@thsa.org

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

3. Filing a Complaint. The THSA will provide the following assistance when a person wishes to file a complaint:

   a. Complaints to the THSA. 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 the THSA, 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 a complaint form, state in clear terms the nature of the complaint, and/or provide any other information necessary to enable the THSA 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 THSA Management. The Contact Person shall forward all written and oral privacy complaints to the applicable Participant and THSA 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 the THSA'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 the THSA Chief Executive Officer, or if appropriate, the THSA Board Chair for sanctions. The THSA shall apply appropriate sanctions to the workforce member(s) in accordance with Article XII of these Privacy Policies.

7. Resolution of Privacy Complaints. The Contact Person may, within a reasonable period of time, 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. The THSA 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. The THSA 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 XII - SANCTIONS

Sanctions			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: *September 23, 2013*	Board of Directors Approval: *September 27, 2013*	Article: *XII*	Version: *1.0*

POLICY

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

PROCEDURE

1. Parties Responsible for Imposing Discipline. The THSA Chief Executive Officer, or if appropriate, the THSA Board Chair will be responsible for determining sanctions for privacy violations.

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

3. Violations That Will Prompt Consideration of Disciplinary Action. The THSA may impose discipline, up to and including discharge and/or restitution, for violations of either these 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. The THSA 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;

[3] 78 Fed Reg. 17, 5580.

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 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 THSA 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, the THSA 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, the THSA 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. The THSA 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 to impose discipline, the identity of the individual whose privacy rights were violated shall be removed to the extent feasible.

7. Documentation of Discipline. The THSA 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.

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

The THSA 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 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 XIII - MITIGATION

Mitigation			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: ~~*September 23, 2013*~~*May 12, 2019*	Board of Directors Approval: ~~*September 27, 2013*~~*November 1, 2019*	Article: *XIII*	Version: *1.*~~*0*~~*1*

POLICY

The THSA shall mitigate any harmful effect known to the THSA of a use or disclosure of PHI by the THSA or any of its subcontractors in violation of the Privacy Standards or Security Standards. Employees of the THSA, 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. The THSA 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 the THSA.

PROCEDURE

1. Report Harmful Effects of Inappropriate Uses or Disclosures to the THSA ~~General Counsel~~. A workforce member of the THSA 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 THSA ~~General Counsel~~ or other appointee responsible for collecting such reports.

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

3. Take Reasonable Steps to Mitigate Harmful Effects. The THSA shall take reasonable steps to mitigate a known harmful effect of a use or disclosure of PHI by the THSA. The reasonable steps may be implemented based on the THSA's prudent judgment, including, without limitation, the THSA'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. The THSA is not required to monitor the activities of its subcontractors; however, if the THSA 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, the THSA 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, the THSA 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 XIV - PARTICIPANT AND SUBCONTRACTOR BUSINESS ASSOCIATE AGREEMENT POLICY

Participant and Subcontractor Business Associate Agreement Policy			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: ~~*September 23, 2013*~~*May 12, 2019*	Board of Directors Approval: ~~*September 27, 2013*~~*November 1, 2019*	Article: *XIV*	Version: *1.*~~*0*~~*1*

POLICY

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

PROCEDURE

1. Participant Business Associate Agreements. The THSA shall enter into a BAA with each of its Participants. To the extent that the THSA negotiates individual terms with individual Participants, this may result in the creation of various, different obligations on the part of the THSA.

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

    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 the THSA's Privacy Officer~~'s General Counsel~~. Any non-routine use or disclosure by a subcontractor that is either reported by the subcontractor or discovered by THSA personnel must be reported to the THSA's General Counsel immediately. The THSA will ensure that any limitations put on its uses and disclosures by its BAA with Participant is included in its BAA with any subcontractors. The following shall be the contact person for the responsibilities addressed in this Article:

        ~~**Anne Kimbol**~~**Privacy Officer**

~~General Counsel~~
Texas Health Services Authority
~~221 E. 9th Street, Ste. 201~~901 S. Mopac Expressway, Building 1, Ste. 300
Austin, Texas 7874~~78701~~
~~(512) 814-0321 (ext. 303)~~512-329-2730
Privacy@thsa.org~~Anne.Kimbol@thsa.org~~

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

c. *Subcontractor's Obligations*. The subcontractor should be able to demonstrate to the THSA that it has procedures in place to assure that it can adequately safeguard PHI. The subcontractor must be able to assist the THSA in a timely manner to ensure that patients served by HIETexas may exercise their 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 the THSA's Participant.

ii. Amend any PHI about the patient that the subcontractor maintains in a designated record set, upon request of the THSA'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 the THSA's Participant.

iv. Comply with all of the THSA'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*. The THSA should notify its subcontractors in writing whenever it changes its policies or procedures in a manner that affects the subcontractor, and 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 the THSA, unless an exception to the minimum necessary rule applies by law and pursuant to the THSA's policies.

f. *Violations by Subcontractor*. If the THSA 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 the THSA'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 XV - DOCUMENTATION, AMENDMENT AND RETENTION OF RECORDS POLICY

Documentation, Amendment and Retention of Records Policy			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: *September 23, 2013*	Board of Directors Approval: *September 27, 2013*	Article: *XV*	Version: *1.0*

POLICY

The THSA 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.

PROCEDURE

1. Documenting Policies and Procedures. The THSA shall document (as applicable for those below-listed provisions to the THSA 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. 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.

    b. 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.

c. De-identification and re-identification.

d. 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.

e. Research.

f. Marketing (optional).

g. Fundraising.

h. Safeguards, including:

i. administrative;

ii. technical; and

iii. physical.

i. Training, including:

i. workforce training;

ii. other educational tools; and

iii. educating patients about their rights and responsibilities.

j. Audits, including:

i. routine internal audits; and

ii. compliance audits by Office for Civil Rights.

k. Receiving and resolving complaints.

l. Sanctions.

m. Mitigation.

n. Agreements with vendors and service providers who are:

i. Business Associates;

ii. trading partners; and

iii. chain of trust partners.

o. Requests for preemption exception.

p. Documentation and record retention.

q. Policy and procedure amendments.

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

The THSA 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. The THSA 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*. The THSA may place the initial responsibility and authority with the Privacy Officer, or some other appointed person, to formulate, adopt, and recommend any changes and amendments to the privacy policies and procedures in these Privacy Policies, or to add policies and procedures as necessary or required by law or regulation. The THSA 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, the THSA 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, the THSA should require such amendment to be performed in as timely a manner as necessary. Adoption of amendments to this Privacy Policy may be effected in the same manner required for adoption of other policies. If the THSA makes any representations to consumers about its policies, and particularly any representations regarding how PHI is used

or disclosed, the THSA 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 the THSA amends a policy and procedure that affects the confidentiality of PHI, it should consider to what extent Participants who are HIPAA Covered Entities 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*. The THSA shall document all amendments to its policies and procedures.

e. *Review (Optional)*. These Privacy Policies shall be reviewed at least annually 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 the THSA. The THSA may adopt temporary revisions to its privacy policies and procedures, prior to board approval, in order to effectively accomplish its business operations.

4. Retention of Documents Demonstrating Privacy Compliance. The THSA shall retain, and may also require its Participants to retain, the policies and procedures provided for in this Article 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.

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 XVI - BREACH NOTIFICATION POLICY

Breach Notification Policy			
Texas Health Services Authority	**Privacy Policies & Procedures**		
Effective Date: ~~*September 23, 2013*~~*May 12, 2019*	Board of Directors Approval: ~~*September 27, 2013*~~*November 1, 2019*	Article: *XVI*	Version: *1.*~~*0*~~*1*

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 THSA, as a Business Associate of the Participant, must notify the Participant in a timely manner in order for proper notification to be given to the individual and HHS. The Participant may also delegate Breach Notification to the THSA in the BAA. The THSA shall consult its Participant BAA and Participation Agreement to determine whether they contain any more specific requirements regarding breaches.

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 THSA 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 the THSA, or a Business Associate of the THSA, 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 the THSA, 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 the THSA, including a Business

Associate, or to an organized health care arrangement in which the THSA 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 the THSA, or a Business Associate of the THSA, 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 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. Therefore, subcontractors of the THSA must properly notify the THSA, so that the THSA may properly notify its Participants who are covered entities, or its Participants who are business associates who are required to give notice to its Participants who are covered entities. The THSA must within the applicable legal time frame for submitting such notice, but in no event longer than sixty (60) days after discovery of the breach, provide a notification to all Participants with individuals likely impacted by the breach. The THSA 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 the THSA as of the first (1st) day on which such breach is actually known to the THSA or, by the exercise of reasonable diligence, would have been known to the THSA. The THSA 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 the THSA.

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 the THSA 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 the THSA to have been, accessed, acquired, used, or disclosed during the breach.

d. The THSA shall supplement the information contained in the notification as it becomes available. The notification required by this Policy shall not include any PHI.

e. The THSA 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 the THSA required by paragraph 2 or an agreement to require the THSA to notify affected individuals on behalf of Participant in the event that a breach of unsecured PHI is discovered by the THSA.

3. Breach Detection and Analysis.

a. The THSA 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 the THSA who discovers the breach must take immediate steps to report the breach to the THSA Privacy Officer~~General Counsel~~.

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, the THSA 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, the THSA 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, the THSA 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;

The THSA 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 the THSA.

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, the THSA 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

The THSA 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, the THSA could determine that the information was not actually acquired by an individual even though the opportunity existed. In contrast, however, if the THSA sent the information to the wrong individual who called the THSA and told the THSA 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.

The THSA 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, the THSA 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*. The THSA shall train all members of its workforce as necessary and appropriate to ensure the THSA's compliance with this Article XVII in accordance with Article XI of these Privacy Policies.

b. *Sanctions*. The THSA shall apply appropriate sanctions, in accordance with the THSA's Article on Sanctions, against members of its workforce that fail to comply with that Article.

c. *Complaints*. Individuals can make complaints concerning this Article in accordance with the Article on complaints in these Privacy Policies.

d. *Documentation*. The THSA shall comply with the Article on documentation in these Privacy Policies and shall document that all notifications are made in accordance with applicable law and these 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").

ARTICLE XVII - SENSITIVE PERSONAL INFORMATION BREACH NOTIFICATION

Sensitive Personal Information Breach Notification			
Texas Health Services Authority	**Privacy Policies & Procedures**		
Effective Date: ~~September 23, 2013~~May 12, 2019	Board of Directors Approval: ~~September 27, 2013~~November 1, 2019	Article: *XVII*	Version: *1.~~0~~1*

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, the THSA 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. The THSA 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 to Individuals.

a. *Timing Requirements*. Following the discovery of a breach of system security, the THSA shall immediately provide written notice to the Participant. THSA shall also make this disclosure to individuals without unreasonable delay and in each case not later than the 60th day after the date on which the THSA determines that the breach occurred. However, the THSA may delay in providing notice if requested by a law enforcement agency that determines that notification would impede a criminal investigation. The THSA 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. The THSA shall consult its Participant BAA and Participation Agreement to determine whether they contain any additional requirements.

b. *Residency of Affected Individuals*. 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 other than Texas, the notice of the breach of system security may be provided under that state's law OR in accordance with this Article.

c. *Methods of Notification*. The THSA 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 the THSA demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the THSA does not have sufficient contact information, the notice may be given by electronic mail (if the THSA has email addresses for the affected individuals); conspicuous posting of the notice on HIETexas.org; or notice published or broadcast on major statewide media.

d. *Deemed Compliance*. Notwithstanding the methods of notification listed above, if the THSA 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, the THSA will be deemed to have complied with the Act if the THSA provides notice in accordance with that policy.

3. Breach Notification Requirements to the Texas Attorney General.

a. In addition to the notification requirements above, the THSA shall also notify the attorney general of the breach not later than the 60th day after the date on which the THSA determines that the breach occurred if the breach involves at least 250 Texas residents.

b. The notification to the attorney general shall include:

i. A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;

ii. The number of Texas residents affected by the breach at the time of notification;

iii. The measures taken by the THSA regarding the breach;

iv. A~~a~~ny measures the THSA intends to take regarding the breach after the notification is made; and

v. I~~i~~nformation regarding whether law enforcement is engaged in investigating the breach.

4. Breach Notification Requirements to the Texas Health and Human Services Commission.

a. When and where appropriate, THSA will

i. N~~n~~otify Texas HHSC immediately upon discovery of a breach;

ii. Follow a documented breach response plan, in accordance with the HHSC DUA; and

~~iv.~~iii. Notify individuals and reporting authorities whose information has been breached at the direction of Texas HHSC.

REFERENCES/CITATIONS

TEXAS BUSINESS & COMMERCE CODE §521.002 §521.053, as amended by SB 1610 (83R) and HB 4390 (86R).

ARTICLE XVIII - PERMITTED USES AND DISCLOSURES

SUBJECT TO APPLICABLE BUSINESS ASSOCIATE AND PARTICIPATION AGREEMENTS

Permitted Uses and Disclosures ***Subject to Applicable Business Associate and Participation Agreements***			
Texas Health Services Authority		**Privacy Policies & Procedures**	
Effective Date: ~~*September 23, 2013*~~*May 12, 2019*	Board of Directors Approval: ~~*September 27, 2013*~~*November 1, 2019*	Article: *XVIII*	Version: *1.*~~*0*~~*1*

POLICY

The THSA may use or disclose the PHI only to the extent authorized under its BAA and Participation Agreement or as otherwise authorized or required under applicable law.

The purpose of HIETexas is to ~~connect Participants to each other and to the eHealth Exchange~~act as a "seamless electronic health information infrastructure to support the health care system in the state and to improve patient safety and quality of care." The THSA~~, through its technology subcontractor InterSystems Corporation,~~ maintains only a minimal amount of PHI in ~~connection with its record locator service~~the form of demographic and administrative information. Because determinations regarding what constitutes a permitted disclosure of PHI occur at the provider level, the THSA will rely on the Participants' compliance with applicable medical privacy law~~, as a signatory to the State-Level Trust Agreement,~~ that the disclosure is permitted or required under state and federal medical privacy law when disclosures of PHI are made through HIETexas.

To the extent that the THSA, through HIETexas, does disclose a minimal amount of PHI solely for its record locator service and log files, the THSA adheres to these policies and procedures on the permitted uses and disclosures of PHI.

The THSA will explicitly comply with the provisions of the HHS DUA, including but not limited to, limiting all uses and disclosures where and when appropriate to the authorized users and authorized purposes (as identified in the HHS DUA) relating to creation, receipt, maintenance, use, disclosure, access or transmission of Texas HHS Confidential Information.

ARTICLE XIX - PERMITTED USES AND DISCLOSURES
APPLICATION OF THE MINIMUM NECESSARY RULE

Permitted Uses and Disclosures ***Application of the Minimum Necessary Rule***			
Texas Health Services Authority	**Privacy Policies & Procedures**		
Effective Date: ~~*September 23, 2013*~~*May 12, 2019*	Board of Directors Approval: ~~*September 27, 2013*~~*November 1, 2019*	Article: *XIX*	Version: *1.*~~*0*~~*1*

POLICY

This policy shall be enforced to limit the use and disclosure of PHI by all THSA 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.

~~The purpose of HIETexas is to connect Participants to each other and to the eHealth Exchange. The THSA, through its technology subcontractor InterSystems Corporation, maintains only a minimal amount of PHI in connection with its record locator service.~~ Because "minimum necessary" determinations occur at the provider level, the THSA will rely on the Participants' compliance with applicable medical privacy law~~, as a signatory to the State Level Trust Agreement,~~ that the disclosure is the minimum necessary required to accomplish the intended purpose of the disclosure.

To the extent that the THSA, through HIETexas, does disclose a minimal amount of PHI ~~solely for its record locator service~~, the THSA adheres to the below-listed procedures on the minimum necessary rule.

The THSA will explicitly comply with the provisions of the HHS DUA, including but not limited to, limiting all uses and disclosures where and when appropriate to the authorized users and authorized purposes (as identified in the HHS DUA) relating to creation, receipt, maintenance, use, disclosure, access or transmission of Texas HHS Confidential Information.

PROCEDURE

1. Uses.

   a. The THSA 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. THSA workforce members' access to PHI shall be solely on a "need to know" basis. THSA 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, the THSA shall develop and implement standard protocols.

b. Non-routine requests for, and disclosures of, PHI shall be reviewed by the THSA Privacy Officer~~General Counsel~~. The THSA 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. The THSA 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 the THSA's available resources, to meet the minimum necessary provisions of the HIPAA final omnibus rule. The THSA shall accomplish this by removing identifiers and removing data fields not necessary to performing the primary purpose of the use or disclosure.

5. The THSA ~~General Counsel~~Privacy Officer 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 the THSA may be used by THSA workforce members to facilitate exchange of information between Participants for treatment, payment, or healthcare operations of Participants in HIETexas. PHI may not be disclosed outside of the THSA unless such disclosure is made to:

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

b. As otherwise Required by Law.

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)

~~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 the THSA's workforce including staff, employees, volunteers, independent contractors, trainees and others who, in the performance of work for the THSA, are under the THSA's direct control and who have access to protected health information ("PHI") maintained, received, or transmitted by the THSA.

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

The THSA 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, the THSA 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 the THSA, I will not at any time during or after my work for the THSA speak about or share any PHI with any person or permit any person to examine or make copies of any PHI maintained by the THSA, or any Participants in HIETexas. 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 HIETexas.

3. Safeguards.

   When PHI must be discussed with other healthcare practitioners in the course of my work for the THSA, 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 the THSA's information systems, and I will take all reasonable measures to prevent the disclosure of my access codes to anyone. I also understand that the THSA 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 the THSA's policies and procedures, completed the training courses offered by the THSA, and shall abide by the THSA's policies and procedures governing the protection of PHI.

5. Return or Destruction of Protected Health Information.

If, as part of my job responsibilities, I must take PHI off the premises of the THSA, I shall ensure that I have the THSA'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 the THSA or destroyed in a manner that renders it unreadable and unusable by anyone else.

6. Termination.

At the end of my employment with the THSA, or when my assignment for the THSA is otherwise terminated, I will make sure that I take no PHI with me, and that all PHI in any form is returned to the THSA 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 the THSA 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 the THSA any unauthorized use or disclosure of PHI by any person. I will report unauthorized uses and disclosures of PHI to the following person/office:

~~**Anne Kimbol**~~**THSA Privacy Officer**

~~General Counsel~~
Texas Health Services Authority
~~221 E. 9th Street, Ste. 201~~901 S. Mopac Expressway, Building 1, Ste. 300
Austin, Texas ~~78701~~78746
~~(512) 814-0321 (ext. 303)~~512-329-2732
~~Anne.Kimbol@thsa.org~~Privacy@thsa.org

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 the THSA'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 the THSA 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

Texas Health Services Authority

Concerns or Complaints Regarding Privacy Practices

The THSA 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 THSA Use Only:

Date received: _____
Received by: _____
Date forwarded to THSA ~~General Counsel~~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.

TEXAS HEALTH SERVICES AUTHORITY
POLICIES
REGARDING THE SECURITY OF HEALTH INFORMATION

Attachment No. 2

Minutes of the August 16, 2019 Board Meeting

TEXAS HEALTH SERVICES AUTHORITY

TEXAS STATE CAPITOL EXTENSION BUILDING
ROOM E2.026
1100 CONGRESS AVENUE
AUSTIN, TX 78701

BOARD OF DIRECTORS MEETING
FRIDAY, AUGUST 16, 2019
10:00 A.M.

TEXAS OPEN MEETINGS NOTICE

The THSA Board of Directors is subject to Texas Government Code, Section 551.021:
"Minutes of Open Meeting Required. (a) A governmental body shall prepare and keep minutes or make a recording of each open meeting of the body. (b) The minutes must: (1) state the subject of each deliberation; and (2) indicate each vote, order, decision, or other action taken."

MEMBERS PRESENT

Shannon Calhoun (Chair), Jonathan Sandstrom Hill (Treasurer), Victoria Bryant, Lourdes Cuellar, Salil Deshpande, Kenneth James, Jerome Lisk, Leticia Rodriguez

MEMBERS ABSENT

Emily Hartmann (Vice-Chair), Paula Anthony-McMann (Secretary), Siobhan Shahan, Carlos Vital, Calvin Green (*HHSC ex-oficio member*), Jeffrey Hoogheem (*DSHS ex-oficio member*)

CALL TO ORDER/WELCOME AND INTRODUCTIONS

Mrs. Shannon Calhoun, THSA Board Chair, called the meeting to order at 10:00 a.m. Chair Calhoun proceeded to review the purpose of the THSA under Chapter 182 of the Health and Safety Code.

BOARD BUSINESS

Consideration of June 14, 2019 Board Hearing Minutes

Approval of Minutes from the June 14, 2019 Board Hearing
BOARD ACTION: Chair Calhoun asked if there were any additions or corrections to the June 14, 2019 hearing minutes. Ms. Leticia Rodriguez made a motion to approve and was seconded by Dr. Victoria Bryant. The motion was approved by a unanimous voice vote.

Consideration of Fiscal Year 2019 Third Quarter Financial Statements:

Approval of THSA's FY 2019 Q3 Financial Statements
Chair Calhoun recognized Mr. Jonathan Sandstrom Hill to review the THSA's 2019 Q3 financial statements through June 30, 2019. Mr. Sandstrom Hill reviewed the financial statements for the board.

BOARD ACTION: Chair Calhoun asked if there was a motion to approve the Financial Statements. Mr. Sandstrom Hill made a motion to approve the Financial Statements. Dr. Salil Deshpande seconded the motion. The motion was approved by a unanimous voice vote.

Consideration of Proposed Fiscal Year 2020 Budget

Approval of Proposed FY 2020 Budget

Chair Calhoun recognized Mr. George Gooch to update members on the THSA's proposed FY 2020 budget. Mr. Gooch reviewed the proposed budget for the board.

BOARD ACTION: Chair Calhoun asked if there was a motion to approve the THSA's proporsed fiscal year 2020 budget. Dr. Salil Deshpande made a motion to approve the budget. Ms. Leticia Rodriguez seconded the motion. The motion was approved by a unanimous voice vote.

EXECUTIVE SESSION

Chair Calhoun advised members that an Executive Session, pursuant to Texas Government Code Section 551.074(a)(1) in Capitol Extension Room E2.022. Ms. Leticia Rodriguez made a motion to approve the Executive Session and was seconded by Dr. Victoria Bryant. The motion was approved by a unanimous voice vote at 10:56 a.m.

Dr. Victoria Bryant made a motion to reconvene into regular session and was seconded by Mr. Kenneth James. The motion was approved by a unanimous voice vote at 12:12 p.m.

PUBLIC COMMENT

Chair Calhoun invited public comment from attendees.

INFORMATION ITEMS

Chair Calhoun asked members if there were any questions or comments regarding normal THSA business items. No action was taken.

FUTURE AGENDA ITEMS

Chair Calhoun advised members of the THSA Board's future meeting schedule. The next Board meeting is scheduled for Friday, November 1, 2019 at 10:00 a.m. in the Texas State Capitol. No vote or action was taken on this item.

ADJOURN

BOARD ACTION: Chair Calhoun asked for a motion to adjourn. A motion was made by Dr. Jerome Lisk and seconded by Dr. Victoria Bryant. The meeting adjourned at 12:15 p.m.

_____

Paula Anthony-McMann, Ph.D, THSA Board Secretary

Attachment No. 3

Current FY 2020 Budget

Attachment No. 4

FY2019 Q4 Financial Statements

Attachment No. 5

Draft State Health IT Strategic Plan

Health Information Technology (Health IT) Strategic Plan

September 2019

Submitted to:

Centers for Medicare and Medicaid Services, Region VI

Submitted by:

Texas Health and Human Services Commission

Contents

Executive Summary

The Centers for Medicare & Medicaid Services (CMS) approved the renewal of the Texas Medicaid 1115 Healthcare Transformation and Quality Improvement Program demonstration waiver on December 17, 2017. Special Terms and Conditions (STC) 39 of the waiver renewal requires the Texas Health and Human Services Commission (HHSC) to develop a Health Information Technology (Health IT) Strategic Plan related to activities in the demonstration that will "link services and core providers across the continuum of care to the greatest extent possible" using Health IT initiatives and strategies.

In Texas, the 1115 waiver governs the Uncompensated Care and Delivery System Reform Incentive Payment (DSRIP) programs. The waiver also represents the authority for most Texas Medicaid managed care, which is the service delivery model for about 93 percent of Texas Medicaid clients. As such a large purchaser of healthcare, Texas Medicaid has the unique opportunity to lay the foundation for a global Health IT approach for the state. Texas Medicaid supports the Texas Health Information Exchange (HIE), five active community-based Health Information Exchanges (Local HIEs) and the health provider community by providing governance and infrastructure to ensure greater interoperability within the state, which follows standards best aligned with Texas Medicaid needs. The Health IT Strategic Plan outlined in this document is designed to implement capabilities complementary to Texas Medicaid and the state's Health IT ecosystem.

Texas is working to increase access to health data across the healthcare continuum, through improvements in provider technologies, such as electronic health record (EHR) systems and strategic use of limited resources to develop methods for establishing interoperability. Access to Medicaid client information supports decision-making by a wide range of entities, including patients, healthcare workers, government agencies and others.

The following three Health IT/HIE strategies detailed in the Texas Health Information Exchange Implementation Advance Planning Document (HIE IAPD) provide the foundation and building blocks for bringing this Health IT Strategic Plan to fruition:

1. **Strategy 1: Medicaid Provider HIE Connectivity** – This strategy is intended to assist Local HIEs with connecting the ambulatory providers and hospitals in their respective areas.
2. **Strategy 2: Texas Health Information Exchange (HIE) Infrastructure** – This strategy aids with building connectivity between the Texas Health Services Authority (THSA), which has a statutory charge to facilitate HIE statewide, and the state's Local HIEs.
3. **Strategy 3: Emergency Department Encounter Notification (EDEN) system** – Texas statewide Health Information Exchange Plan promotes Local HIEs connecting hospitals to their information technology systems and exchanging Admission, Discharge, Transfer (ADT) messages.

This Health IT Strategic Plan discusses how Medicaid managed care can be leveraged to inform the transition to value-based care as a growing proportion of managed care organization (MCO) contracts with providers embrace alternative payment models (APMs). As Medicaid MCO payment models change, health information sharing across the state's Health IT ecosystem becomes more relevant. Texas Medicaid also has several managed care oversight initiatives underway that relate to information sharing, such as a focus on continuous organizational improvement and increasing transparency between providers and members.

Through this Health IT Strategic Plan, HHSC demonstrates compliance with STC 39. STC 39 requires the Health IT Strategic Plan to describe the state's existing Health IT environment and develop an approach to support the following capabilities in furtherance of the programmatic objectives of the demonstration:

1. **C-CDA Format** - Electronic exchange of clinical health information via Consolidated Clinical Document Architecture (C-CDA), when multiple providers provide coordinated care to a client.
2. **Master Patient Index** - Access to a comprehensive Medicaid enterprise master patient index that supports the programmatic objectives of the demonstration.
3. **Provider Directory** - A comprehensive Medicaid service provider directory strategy that supports the programmatic objectives of the demonstration.
4. **Care Coordination** - Improved coordination and integration between Medicaid behavioral health, physical health, home and community-based providers and community-level collaborators through the adoption of provider-level Health IT infrastructure and software.
5. **Care Quality** - A Comprehensive Health IT-enabled quality measurement strategy that supports the collection of data necessary for Texas to monitor and evaluate the demonstration's programmatic objectives.

This Health IT Strategic Plan defines achievable milestones for Health IT adoption by Medicaid service providers, plans for the exchange of clinical health information related to Medicaid clients statewide and advances the standards identified in the "Interoperability Standards Advisory—Best Available Standards and Implementation Specifications" (ISA).

This plan provides background information, including detailing Texas Medicaid's Health IT goals, providing an overview of the Healthcare Transformation and Quality Improvement Program Waiver and detailing the strategic plan development activities. This plan then highlights the findings from using CMS' "1115 Health IT Toolkit,"[1] as directed by STC 39, in conducting an assessment of seven key Health IT topic areas. Finally, the plan includes goals and milestones for Health IT in furtherance of the programmatic objectives of the demonstration.

Texas HHS Vision and Mission and Medicaid Health IT Goals

Texas HHS' vision is: "Making a difference in the lives of the people we serve" and the mission is: "Improving the health, safety and well-being of Texans with good stewardship of public resources."

The Health IT Strategic Plan supports this vision, mission and goals of the Texas Health and Human Services agencies as well as those of the Medicaid and CHIP Services Department. The plan provides a roadmap for improving the health and well-being of our citizens by identifying actions and capabilities using information from the Texas Health IT ecosystem. The plan focuses on increasing the adoption of certified EHR systems, particularly among providers not included in previous federal incentive programs; connecting Texas providers to Local HIEs and leveraging clinical and non-clinical data, data analytics, telemedicine and telehealth to facilitate improved outcomes and care coordination.

Texas Medicaid has developed the following Health IT goals specific to the 1115 Waiver:

1. Incorporate Health IT as a foundational component for the Medicaid managed care delivery model, procurement and HHSC contract oversight efforts.
2. Support the development and maintenance of a coordinated care delivery system by facilitating the timely exchange of clinical, health risk and other data among Texas Medicaid stakeholders.
3. Support transition to value-based models across managed care and providers by:

[1] CMS, in coordination with the Office of the National Coordinator (ONC) for Health IT, has created a series of toolkits and resources for Medicaid focused on health information exchange, Health IT and interoperability. "1115 Health IT Toolkit" materials accessed July 17, 2019 at: https://www.healthit.gov/topic/advancing-interoperability-medicaid

   a. Expanding the use of metrics that integrate administrative, clinical, relevant health risk and other data.
   b. Improving the timely availability of actionable information for decision making.
   c. Translating Health IT best practices from the DSRIP program into managed care.
4. Promote MCOs' use of Health IT to manage member healthcare and related needs, with an emphasis on prevention.
5. Promote Medicaid provider connectivity to the overall Texas Health IT ecosystem.

Healthcare Transformation and Quality Improvement Program Waiver Background

In December 2011, Texas received approval for a Section 1115 Medicaid demonstration waiver to expand existing Medicaid managed care programs statewide while preserving certain safety net provider funding and promoting health system transformation. The Healthcare Transformation and Quality Improvement Program Waiver successfully enabled Texas to expand the STAR and STAR+PLUS Medicaid managed care programs statewide and established the following two funding pools:

1. The Uncompensated Care Pool, which allowed for payments for the unreimbursed costs of services, provided to Medicaid clients and uninsured individuals.
2. The DSRIP Pool, which initially enabled providers participating in 20 Regional Healthcare Partnerships (RHPs) to receive incentive payments for projects, and was designed to promote healthcare infrastructure development and implement program innovation and redesign.

In December 2017, CMS approved an extension of the demonstration for five years through September 30, 2022. Texas' objectives for the demonstration renewal are to:

- expand risk-based managed care to new populations and services;
- support the development and maintenance of a coordinated care delivery system;
- improve outcomes while containing cost growth; and
- transition to quality-based payment systems across managed care and providers.

The demonstration extension represents an evolution from the initial waiver terms as Texas Medicaid managed care now includes:

- additional programs and services;
- a narrowing of the definition of uncompensated care to charity care only; and
- a shift in the focus of the DSRIP program from individual provider projects to more strategic efforts aimed at provider system-level performance measurement and improvement.

The following information provides a brief history on the elements of the demonstration with the closest ties to Health IT – the Medicaid managed care expansion and DSRIP.

Medicaid Managed Care Expansion

For the past 25 years, Texas has gradually transitioned Medicaid from fee-for-service reimbursement to a managed care system that holds health plans accountable for producing value. Under the managed care system, HHSC contracts with managed care organizations (MCOs) competing within 13 service delivery areas and pays a per member per month rate, called a capitation rate or premium, to coordinate care and reimburse providers for health services provided to Medicaid or CHIP members enrolled in their plan.

Texas Medicaid managed care includes the following statewide programs covering the noted populations:

- STAR – children, newborns, pregnant women and some parents with low incomes;
- STAR+PLUS – adults who have disabilities, are age 65 or older or have breast and/or cervical cancer;
- STAR Health – children and youth who receive Medicaid because they either currently are or formerly were in the conservatorship of the state;
- STAR Kids – children and youth age 20 or younger who have disabilities; and
- Children's Medicaid Dental Services – most children and youth under age 21.

The managed care model has become the centerpiece of the state's strategy to promote value-based care in Medicaid. As of November 2018, about 93 percent of Texas Medicaid and CHIP clients received services through risk-bearing MCOs, making Texas a national leader for delivering healthcare through a value-based model to people with low income or disabilities.

Delivery System Reform Incentive Payment (DSRIP) Program

Since 2012, 300 providers have earned over $16 billion (all funds) through DSRIP for increasing access to care, piloting care innovations and improving health outcomes. DSRIP providers include hospitals (public and private), community mental health centers, local health departments and physician practices - mostly affiliated with academic health science centers.

In demonstration years one through six, DSRIP providers earned funds by achieving process and outcome measures related to projects they chose from an approved "menu" of initiatives, designed to either develop infrastructure or test healthcare innovations. The most common focuses of DSRIP projects over the first six years of the program were:

- Behavioral Healthcare (mental health and substance use care);
- Primary Care (Expansion/Redesign/Patient Centered Medical Homes);
- Patient Navigation/Care Coordination/Care Transitions;
- Chronic Care Management; and
- Health Promotion/Disease Prevention.

An early success of the DSRIP program was the establishment of 20 Regional Healthcare Partnerships (RHPs) covering the state, which led to increased local collaboration to identify and address priority community healthcare needs. Activities are underway in many regions to further connect MCOs and DSRIP providers to better coordinate their efforts. These sorts of connections among healthcare providers and between healthcare providers and MCOs either benefit from current Health IT adoption or could be further enhanced through future advancements in Health IT adoption, including standards-based health information exchange.

The DSRIP funding pool was extended in the latest waiver renewal under a model that shifts the focus of delivery system transformation from individual provider projects to more strategic efforts aimed at provider system-level performance measurement and improvement. The current DSRIP funding ends October 1, 2021. Transition planning is under way to further develop delivery system reform efforts after DSRIP ends. This Health IT Strategic Plan is a crucial component to identify areas where Health IT is already supporting the objectives of the demonstration as well as additional opportunities for advancing care coordination and other quality improvement efforts.

Strategic Plan Development Activities

The development of the Health IT Strategic Plan began with review and consultations regarding the Texas State Medicaid Health IT Plan (SMHP), SMHPs from other states and the 2015 Texas Medicaid Information Technology Architecture (MITA) State Self-Assessment (SS-A). The next Texas MITA SS-A is in progress as of the development of this plan.

Additional early information-gathering activities included meetings and discussions in 2018 with a broad range of Texas Health IT stakeholders and HHSC leadership and staff. Input was received from HHS advisory groups, Health IT stakeholders, MCOs, providers and HHS staff. In June 2019, an overview of draft milestones was provided at a public meeting of the HHSC e-Health Advisory Committee (eHAC), where committee members provided preliminary feedback. Further discussions regarding the information presented were held with workgroup members of eHAC.

HHSC recognizes strong collaboration is required to increase the flow of clinical data in the state. Internally as well as in HHSC discussions with healthcare stakeholders about Health IT in Texas, a consistent theme in stakeholder feedback was the limited exchange of health information. Additional concerns included the items listed below:

- The low percentage of Medicaid ambulatory providers that are connected to health information networks;
- Lack of trust among providers and payers;
- Lack of standardized processes for connectivity;
- Lack of standardized approaches to value-based purchasing;
- The low percentage of long-term care, behavioral health and home and community-based service providers using electronic health records and connected to health information networks; and
- The cost and administrative barriers providers face regarding participation in the Health IT ecosystem.

Texas HHS agencies have aligned in their pursuit of strategies to advance Health IT, improve care coordination and reduce provider burden. This includes several connectivity strategies, modernization of HHS' infrastructure interfaces to its Health IT information systems, implementation of a provider management and enrollment system, ongoing enterprise data governance efforts building patient and provider master indices, updating of the registry systems supporting clinical data exchange with providers and using clinical data to provide HHS staff with additional tools to aid and support program innovation.

1115 Health IT Toolkit Health IT Topic Discussion

This strategic plan used the seven Health IT topics outlined in the CMS "1115 Health IT Toolkit"[2] to assess Health IT considerations. This section of the strategic plan provides an overview of the considerations for each Health IT topic followed by the results of HHSC's assessment for each topic area.

[2] "1115 Health IT Toolkit" materials accessed July 17, 2019 at: https://www.healthit.gov/topic/advancing-interoperability-medicaid

Overview of Health IT Topics

This section provides a brief overview of considerations for each Health IT topic identified in the "1115 Health IT Toolkit." Texas has considered the principles and guidelines outlined in the CMS toolkit to align with the Health IT Strategic Plan.

The Use of Standards in Health Information Technology Procurement:
Contracts with providers, vendors and other healthcare entities should require the use of messaging and data standards specified in the ISA maintained by the Office of the National Coordinator (ONC) for Health IT.

Leveraging State Health IT Ecosystem:
Where practical, new or expanded services using Health IT should leverage previous investments in health information technology. For example:

- No unnecessary duplicative networks should be established;
- Where practical and appropriate back-up systems exist, health information exchanges should be leveraged to facilitate data exchange; and
- Technology standards for telemedicine should be standard across programs to facilitate re-use of equipment.

Accountable Oversight and Rules of Engagement for Health IT and Health Information Exchange (a.k.a. Governance):
Governance of health information exchanges, selection of standards for exchange and quality standards must be managed in as transparent a manner as possible. Collaboration in governance-related activities should be promoted.

Identity Management, Provider Directories and Attribution:
Health IT can be used to manage individual patients' identities. Accurate patient identification and matching across disparate systems is critical to minimize patient risk and improve the efficiency of healthcare delivery, inclusive of care coordination. Provider directories can be established and used to facilitate data exchange and reporting, payment services and assisting patients in identifying potential care providers. Using a provider directory enables longitudinal tracking of provider behavior as well as facilitates matching provider-related records across information systems.

Promoting and Funding Provider Health IT Adoption and Use:
Appropriate technical and financial assistance for healthcare providers helps to promote the adoption and use of Health IT. Examples of relevant activities include, but are not limited to:

- Providing funding supporting the adoption and use of Health IT, including EHR technology;
- Providing grants for purchasing/using technologies supporting telehealth/telemedicine; and
- Conducting programs focused on encouraging providers to use health information technology.

Advancing Use of Health IT to Support Quality Measurement:
The use of health information technology should support improved quality measurement. This includes the exchange of quality measures between providers and other parties and the transparency of quality measure data to the public. Quality measures may be used by providers, payers and patients to understand, select and improve healthcare options.

Health IT and Service Delivery:
Ultimately, effective Health IT must deliver services that improve the patient experience of care, improve the health of individuals and communities, lower costs and are valued by patients as well as the professionals and organizations accountable for providing and coordinating their care. Examples of successful Health IT services include, but are not limited to, providing the following:

- An interoperable health registry to reduce administrative activities required to comply with applicable law;
- An interoperable health registry that supports bi-directional flow of information to facilitate the coordination of care;
- Near real-time alerts on meaningful healthcare events such as patient admissions, discharges and transfers involving hospital emergency and inpatient departments;
- Technology-based tools that enable providers and/or patients to better manage an individual's health;
- Computer-based support for decision-making to healthcare providers; and
- A patient portal or messaging support to enable patients to access their own health records.

Health IT Topic: The Use of Standards in Health Information Technology Procurement

HHS agencies have a long history of using systems that support standards-based interoperability with trading partners. A combination of federal laws, state laws and regulations have shaped the Health IT infrastructure. Both HHSC and the Department of State Health Services (DSHS) have implemented technologies in response to national directives, whether it was a highly choreographed revision of all healthcare stakeholder systems for compliance with *International Classification of Diseases, 10th Revision* (ICD-10) or the implementation of commercially available, off-the-shelf software provided by the Centers for Disease Control. Texas HHS strategically recognizes Health IT as foundational to advances in many of its business areas and that a standard-based approach maximizes interoperability with the Certified EHR Technology (CEHRT) technologies used across the Health IT ecosystem.

H.B. 2641, 84th Legislature, Regular Session, 2015 required that information systems planned or procured on or after September 1, 2015 and used by a Texas Health and Human Services agency to send or receive protected health information to and from healthcare providers use applicable standards and be interoperable with each other. H.B. 2641 aligns with federal legislation and promotes the use of certified electronic health record technology as well as requires the use of standards such as those included in the ISA.

Modernization procurements associated with Medicaid Management Information Systems (MMIS) must adhere to use of standards in Health IT platforms for all secure web services, file and data transmission. The same requirements apply to Health IT systems related to a distributed Service Oriented Architecture which is essentially a collection of services that communicate with each other where communication can involve either simple data passing, or two or more services coordinating some activity and Electronic Data Interchange (EDI), which is the electronic interchange of business information using a standardized format.

HHS' Current MMIS EDI System

The current Texas Medicaid EDI system is a Council for Affordable Quality Healthcare CORE-compliant, standards-based gateway, for receiving, validating, tracking and routing transactions. The system is composed of reusable business and technical services, with business processes orchestrating the flow. Common file tracking services are used across all subsystems and common reprocessing and alerts are configured for all business processes.

Supported Transaction Types, Standards and Methods

HIPAA X12 Transactions:

- X12 837 I/P/D (Acute and Long-Term Care Claims)
- X12 837 I/P/D (Acute and Long-Term Care Encounters)
- X12 837P (Medical Transportation Encounters)
- 270/271 (Eligibility Benefit Inquiry and Response)
- 276/277 (Claim Status Request and Response)
- 277CA (Claim Acknowledgement)
- 835 (Claim Payment/Advice)
- 278 (Request for Review and Response)
- 275 (Authorization Attachment)

Pharmacy Transactions

- NCPDP PA23 (Medicaid Pharmacy Encounters)
- PDE (Medicare Prescription Drug Event)
- HL7 (Health Level 7)
- Claims-based Electronic Health Record
- HITSP CDA C32 - Clinical Documents
- ITI-41 (Provide and Register) - Claim/Encounter
- ITI-43 (Retrieve Document Set) – Claim/Encounter

Use of Common Standards in Healthcare

Some common standards used in healthcare today are: Health Level 7 (HL7); Fast Healthcare Interoperability Resources (FHIR); Digital Imaging and Communications in Medicine; and North American Association of Central Cancer Registries Version 15. All these standards are included in the ISA. HHSC addresses standards in a biennial report on interoperability as required by H.B. 2641, 84th Legislature, Regular Session, 2015. *Interoperability for Texas: Powering Health 2016*[3] identifies some of the national and international standards development organizations involved in standards used in healthcare.

The HL7 standard is structured to accommodate various types of messages transfers using different implementation guides. There are different HL7 structures for a broad range of purposes, including electronic laboratory reporting and immunization. Even though these HL7 message types differ, the healthcare industry understands the different subtypes as parts of a broader system. HL7 is leading a project known as the HL7 Da Vinci Project with vendors, providers and payers to promote industry wide standards and adoption through the development of unique solutions to improve care. One area of focus is automating support for prior authorizations. The goal is to standardize the information exchange required between payers and providers for payer authorizations.

The FHIR standard is a new specification from HL7, based on emerging industry approaches, but informed by years of lessons around requirements, successes and challenges from previous experience with standards. FHIR can be used as a stand-alone standard or can also be used in conjunction with other standards. FHIR is easy to implement compared to most standards presently used in the healthcare industry.

[3] *Interoperability for Texas: Powering Health 2016.* HHSC. Accessed July 18, 2019 at: https://hhs.texas.gov/sites/default/files/documents/laws-regulations/reports-presentations/interoperability-texas-powering-health-2016.pdf.,

As the state's public health agency, DSHS operates numerous public health registries that contain valuable clinical information used to understand, plan for and manage health services and needs across Texas. Each of the registries use standardized messages, usually in formats specified by federal partners, HL7 or other national standards development organizations. Data for several systems are received via implementations of Orion gateway services. In other cases, data may be exchanged through standard messages directly with receiving systems or through web-based data entry. More information regarding DSHS may be found in Appendix C.

Health IT Topic: Leveraging the Texas Health IT Ecosystem

This Health IT Strategic Plan fully leverages Health IT infrastructure already built and in use by internal state and external healthcare entities. The 1115 demonstration is building on the existing Health IT infrastructure and initiatives, including findings of the MITA state self-assessment, state SMHP and active IAPDs. An example of one such initiative, and referenced subsequently in this document, is the Medicaid Electronic Health Record Incentive/Promoting Interoperability (PI) Program established via the Health Information Technology for Economic and Clinical Health (HITECH) Act. The EHR Incentive/PI Program has allowed HHSC to provide more than $864 million in federal EHR incentive funding to more than 10,000 providers and hospitals since the inception of the program in 2011. This approach ensures Texas' tax dollars are judiciously spent and invested; as well as, ensures Federal Medical Assistance Percentages (FMAP) funds are used in accordance with CMS rules and regulations. Texas adopts national and state best business practices and leverages systems and experience from other states who also use FMAP funds. Policy and standards adopted Ein Texas are commonplace in the healthcare industry. Specific examples of how this works include:

- Many state and local for-profit and nonprofit HIEs that support bi-directional exchange across providers are currently operational and committed to the statewide exchange of clinical data and ADT data;
- MCOs, as Medicaid payers charged with facilitating care coordination for their members, work directly with hospitals and providers to provide funding and technical assistance for connectivity to HIEs and EHR interoperability for added value services related to health data exchange;
- HHSC, the state's designated entity for coordinating interstate and intrastate health information exchange, signed a contract in May 2019 with THSA to build infrastructure to connect Texas' HIEs; and
- National networks (e.g., CommonWell, eHealth Exchange, etc.) with products that support interoperability or certified EHR technologies are motivated to leverage existing data highways to propagate and share data.

Texas' Health IT ecosystem consists of a combination of public and private payers, professional entities, providers, associations and HIEs at various stages of maturity and connectivity. Since 2006, the Texas Legislature has passed laws supporting Texas Medicaid and other health agencies strengthening the use of Health IT and aligning with federal initiatives. Appendix A of this plan provides a chronology of Texas legislation supporting health information exchange.

Health IT Exchange Barriers

Like every other state, Texas has challenges with data sharing across the healthcare provider community. The lack of interoperability across the varying CEHRT products used by providers makes true data sharing an ongoing challenge. Providers continue to feel overburdened by quality reporting requirements in the Promoting Interoperability Program as well as other CMS quality programs.

Other barriers to provider participation include the costs to build interfaces to trusted networks (HIEs), and the hesitancy of providers to share clinical data with payers and other providers. Some providers fear that the data they share could be used against provider and patient interests, such as fear over payer intervention in care decisions or that the information they share could influence patient premiums.

Trust potentially can be built among the provider community and payers by bringing value through provision of clinical data and ADT to automate payer processes, such as prior authorizations. This example underlines the improvements that can result from transparency and information sharing between provider and payer. Additionally, value-based payment models could shift providers' view of claims data and lessen the reticence to payer participation in HIE.

Health IT Ecosystem Strategies

Some of the strategies Texas is pursuing to address obstacles include working around the cost barriers of connectivity (see the following discussion of HIE IAPD Strategy 1: HIE Connectivity) and building incentives for data sharing through Medicaid managed care requirements for alternate payment models between health plans and providers. With the passage of the 21st Century Cures Act in FFY 2017, there has been a succession of federal rules strengthening the interoperability requirements of Health IT products and services. Current and proposed rulings promote CEHRT product offerings and information exchange capabilities that make interoperability accessible for a wider reach of healthcare providers. Texas' Health IT strategies align with federal laws and rules, enabling the state to fully benefit from these recent advances in interoperability.

Texas recognizes that public and private Health IT proponents must strategically focus and collaborate to ensure the state has not moved from paper to electronic silos. Texas also recognizes that it is important to continue to promote the benefits of information sharing in healthcare.

State of Health IT and HIE opportunity in Texas

Texas has multiple Health Information Exchanges (HIEs) that are national, state, local or aligned based on EHR products. Participants in HIEs are primarily hospitals or large provider groups. Texas has a statewide framework for exchange, THSA, that accounts for connectivity to the national HIE networks. Texas' plan to implement electronic HIE statewide is market-based and community-driven. To foster HIE growth and adoption across the state, THSA provides ongoing strategic support to Local HIEs. THSA has made available a set of shared services, referred to as HIETexas. One of the most significant benefits of joining HIETexas is the HIE-to-HIE connectivity between authorized HIEs in Texas and across the country.

During Hurricane Harvey, there was a need to offer query-based HIE to assist in the recovery efforts by allowing patients' health information to be available. This access to data proved to be invaluable during the disaster response activities.

Discussion of the strategies within the HIE IAPD that follow demonstrate how THSA will play a major role in services that are essential for ensuring the delivery of health information, such as ADT messages on Medicaid members and updates to clinical registries.

HIE IAPD Strategy 2: HIE Infrastructure

This strategy aids with building connectivity between THSA and the state's Local HIEs and other authorized entities. Funding is used to implement systems to benefit Medicaid's goals of supporting Medicaid client data collected by the Local HIEs. These activities continue with the THSA contract.

This strategy teams HHSC and THSA to develop and implement projects that make HIE services available statewide and continue to enhance state-level shared services. Projects include, but are not limited to:

- Implementation of an HL7 integration engine;
- Implementation of a Master Patient Index related to HIE;
- Implementation of an audit and logging system to monitor all data flow pertaining to Medicaid's HIE IAPD Strategies 1 and 3, regarding provider connectivity and EDEN;
- Implementation of an Administrative User Interface and statistical dashboard for Medicaid to monitor data flows pertaining to HIE IAPD Strategies 1 and 3;
- Configuration of implemented systems supporting Medicaid's HIE IAPD Strategies 1 and 3;
- Maintenance of systems implemented in support of Medicaid's HIE IAPD Strategies 1 and 3, for the term of this IAPD;
- Integration required with Local HIEs to assist them in connecting to THSA in support of Medicaid's HIE IAPD Strategies 1 and 3; and
- Integration work necessary to deliver required data to Medicaid.

This project supports fundamental, statewide infrastructure necessary for exchange of HL7 v2 and CDA-based documents. This functionality promotes the following Promoting Interoperability measures:

- Lab results;
- Transitions of care;
- Immunization registry reporting;
- Electronic lab reporting to public health;
- Syndromic surveillance; and
- Reporting to specialized registries.

HIE IAPD Strategy 3: Emergency Department Encounter Notifications (EDEN)

This strategy establishes the EDEN system – Texas' statewide Health Information Exchange Plan, which provides the ADT processing infrastructure used by hospital systems to exchange ADT data between HIEs or hospitals via THSA when a hospital does not connect directly to a HIE. Medicaid clients' admission, discharge or transfer status will then be transmitted to Texas Medicaid, MCOs, primary care physicians (PCPs) and other care team members. Information about hospital admissions, discharges and transfers are of great value to PCPs for care coordination.

Current emergency department (ED) systems do not always support the push/sharing of ADT messages/notifications data outside the hospital's system for a multitude of reasons. Hospital systems are sometimes reluctant to connect to a Local HIE that also supports a competing hospital system. Since hospitals' provision of ADT messages is voluntary, HHSC intends to increase the likelihood of ADT message transmission adoption by building the ADT processing infrastructure at the statewide level. Once enabled, hospitals will push the ADT messages to their respective HIEs or when needed, directly to THSA.

THSA receives a standardized notification message comprised of elements containing the patient's name, entity of service and date/time of when the admission, discharge or transfer occurred. These notifications are then forwarded to Texas Medicaid, MCOs and/or to HIEs that have partnered with Medicaid to use notification data for care coordination activities. Diagnosis and admissions data is valuable to care coordination and allows MCOs to automate prior authorizations, which is a key benefit for both MCOs and hospitals.

Texas Medicaid will direct funding toward obtaining timely encounter notifications via HL7 ADT data streams from hospitals. Other states have shown beneficial effects of providing alerts to PCPs and other care team members when a patient enters an ED. Texas Medicaid seeks to reduce inappropriate ED use, by educating patients on non-emergent ED alternatives, and provide improved follow-up care. Gathering timely ADT data from EDs and publishing alerts to care team members will facilitate these goals.

HHSC aims to build ADT processing infrastructure complementing HIE notification systems, but on a standardized, statewide scale. The systems implemented by THSA will act solely as a data brokerage, supplying encounter notifications based upon patient matches found in ADT data-streams submitted by hospitals.

This EDEN strategy is complemented by the HIE IAPD Strategy 1, which provides funding for HIEs to connect hospitals, providing HL7 clinical data feeds necessary for EDEN.

Clinical Data and the Integration and Data Exchange Center of Excellence

DSHS, in partnership with HHSC, has been working to establish an Integration and Data Exchange Center of Excellence (iCoE) technology service as a primary point of exchange between Texas' health and human services system and healthcare providers across the state. Based on a commercial-off-the-shelf integration engine, the iCoE is evolving to support the exchange of messages for a broad range of systems, including public health registries, such as syndromic surveillance and routing and storing them to their appropriate destinations. Using a single "front door" makes it easier for providers to maintain connections with the state's systems and reduce the amount of time and effort spent on addressing technology issues. Governance and security processes are in place to minimize the risk of unintended exposure of patient data.

THSA is a central iCoE connection point for statewide clinical data from Medicaid providers linked to HIEs. HHSC's plans are to leverage the capabilities of the iCoE for anticipated large volumes of clinical data transmitted from Medicaid providers including ADT data, other clinical data and lab reports for Medicaid clients.

DSHS is transforming its information systems to use the iCoE. As each DSHS system that relies on patient data is replaced or undergoes a major overhaul that includes interoperability with other systems, the iCoE is reviewed as part of the IT governance process. Concerns about using the iCoE include funding and the time required to modify commercial-off-the-shelf systems to use the iCoE service. Some systems are not modular and may be complicated to integrate.

While most messages are expected to be received from providers in the appropriate industry-standard format for the relevant systems, the iCoE has the capability to transform messages from one format to another and ensure messages have the appropriate content. Leveraging the iCoE will further reduce provider burden by enabling them to use one connection point to send or receive clinical data from Texas HHS. Both HHSC and DSHS will continue to transition external interface capabilities to the iCoE to streamline data exchange and reduce unnecessary, duplicative connections for providers.

Health IT Topic: Accountable Oversight and Rules of Engagement for Health IT and Health Information Exchange (a.k.a. Governance)

Health IT Governance facilitates the appropriate use and secure exchange of health information in Texas. Enacted through policies, processes and practices, the state has instituted a set of governance bodies that offer guidance, establish standards and provide oversight for public and private entities operating in the Health IT space. The following section describes the roles and responsibilities of these organizations.

Texas Health Services Authority

THSA, established by the Texas legislature, with Chapter 182 of the Health and Safety Code, operates a set of shared services called HIETexas, has a governance structure that enables trusted and secure connections between it and the Local HIEs and may connect to national networks such as the e-Health Exchange, Carequality and/or Commonwell. It requires its participant members to operate in accordance with privacy and security rules that are aligned with Health Insurance Portability and Accountability Act (HIPAA) and other relevant federal and state statutes and rules. THSA's governor-appointed board is responsible for decision making with regards to the policies and operations of the shared services THSA provides to its members. The board intends to regularly review performance and utilization reports to ensure services align with the needs of the Texas Health IT ecosystem. The Local HIEs, HHS agencies and members of the healthcare community are represented on the THSA board. The THSA Texas State HIE Plan details more about the THSA structure, plan and HIETexas.[4]

For statewide activities, HHSC and DSHS are active participant members on the board of the THSA. The HHS system has an internal policy for the exchange of clinical data to use when applicable national standards are identified by the ONC, ensuring compliance with state and federal laws and rules. State legislation and internal policy also directs information systems procured, planned or built after September 1, 2015 that exchange clinical data with providers to enable pathways through state and Local HIEs, minimizing the number of connections a provider is required to use for exchanging data with HHS agencies.

The Local HIEs also have a governance structure. Each of the HIEs are overseen by a board that approves their policies and procedures and reviews their operations. Participant users must also demonstrate and agree to abidance of privacy and security rules.

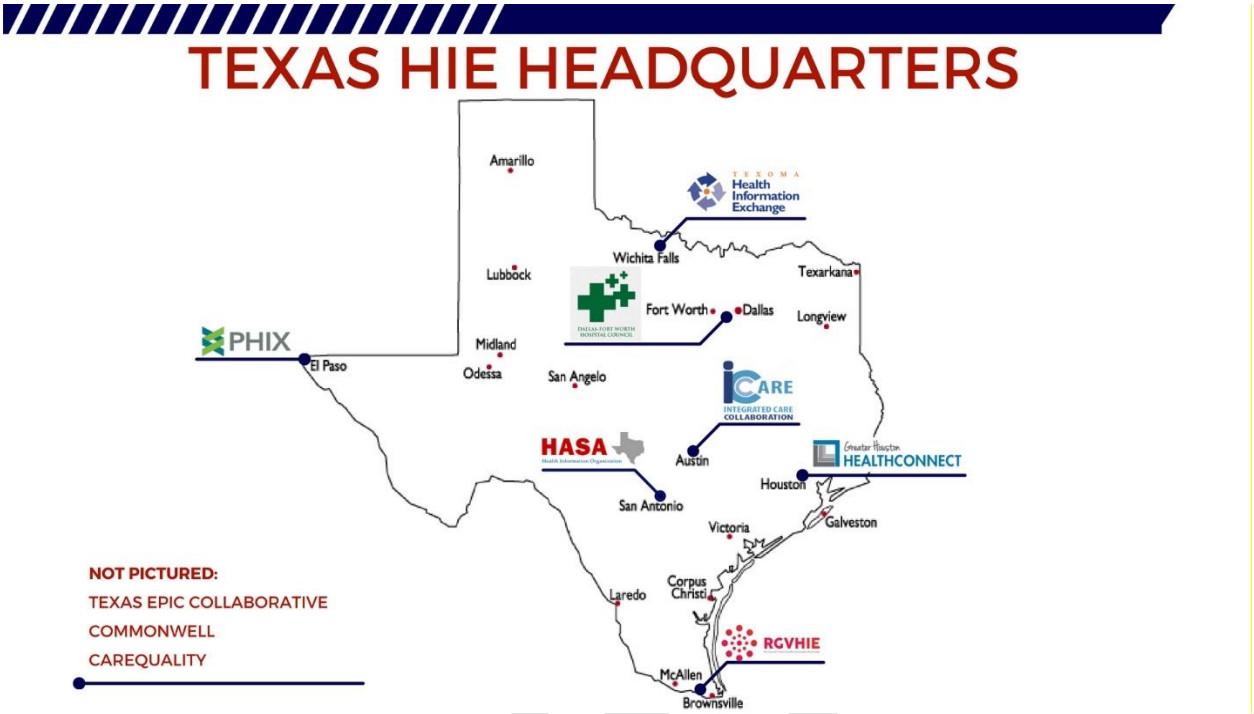
This governance structure is critical as Texas navigates toward the U.S. Core Data for Interoperability (USCDI) and its proposed expansion process aim to achieve the goals set forth in the 21st Century Cures Act by specifying a common set of data classes that are required for interoperable exchange and identifying a predictable, transparent and collaborative process for achieving those goals.

The 21st Century Cures Act contains several requirements aimed at improving interoperability in healthcare and information exchange. As the government builds out the Trusted Exchange Framework and Common Agreement (TEFCA**)** more states have the opportunity of working together to meet national interoperability initiatives and standards. As states join into interoperability partnerships, governance becomes more critical as the foundation for decision making and strategic direction.

Texas has a multi-layered system of governance that complements its Health IT ecosystem design. The following diagram illustrates how governance organizations in Texas work together to maximize interoperability. Further, it shows how Medicaid's participation in a multi-payer, multi-stakeholder governance structure promotes the sharing and interoperability of Health IT.

[4] *Texas State HIE Strategic Plan* accessed July 18, 2019 at: http://www.thsa.org/hie/state-hie-plan/

The Texas Network of Networks



e-Health Advisory Committee

In 2009, the Texas Legislature established the Electronic Health Information Exchange System Advisory Committee to implement HIEs in Texas (H.B. 1218, 81st Legislature, Regular Session). In 2015, after an agency-wide restructuring of advisory committees, the eHAC, was established to advise HHS leadership on activities that could advance Health IT adoption and use in Medicaid. Members of eHAC include: healthcare stakeholders from the academic, industrial and medical professions; as well as other state agencies; health information exchanges and associations.

A key objective of eHAC is to ensure Medicaid Health IT is interoperable with broader statewide infrastructure. To this end, eHAC counsels HHSC on the development and implementation of the HIE system and related issues, including: data to be included, presentation of data, useful measures for quality of services and patient health outcomes, federal and state laws regarding privacy of private patient information, incentives for increasing adoption and use and data exchange with HIEs.

Past eHAC recommendations include the following:

- Incorporate the ONC's Patient Unified Look-up System for Emergencies (PULSE) into the state's disaster response protocols;
- Use of the HIETexas platform, when applicable, to communicate and collaborate with trading partners and HIEs to increase Health IT adoption and use among providers;
- Enable provider access to the state's prescription drug monitoring program through HIEs to help combat the opioid epidemic; and

- Adopt additional communication methods based on stakeholder surveys and research of the constituent groups' messages.

HHSC's internal governance structure also considers eHAC input in the decision-making process regarding Health IT products, including telemedicine, telehealth and home telemonitoring.

The Office of eHealth Coordination (OeHC)

OeHC was established in 2010 to serve as the single point of contact in HHS for health information policy and state funding opportunities under the HITECH Act.

Currently, OeHC coordinates health technology initiatives that exchange protected health information across the HHS system and promotes the use of CEHRT in discussions across the state with healthcare stakeholders.

HHS Enterprise Data Governance

HHS agencies follow a data governance policy implemented by the Chief Data and Analytics Officer (CDAO). The CDAO leads the Center for Analytics and Decision Support and resides within the Office of Performance division. In addition to being responsible for general data and analytics strategies implemented at HHS, the CDAO runs the Enterprise Data Governance (EDG) program, which identified five project tracks to implement Medicaid-focused data governance solutions.

The following table lists and describes the various tracks:

EDG Track	Purpose
Data and information management (DIM)	The DIM track is to implement an enterprise master data management (MDM) system for use across the Health and Human Services (HHS) system.
Data quality and standards (DQS)	The DQS track, which includes claims, encounter and clinical data, ensures that the HHS system can measure the data quality within key HHS systems and make necessary recommendations to improve data quality through the creation of data standards.
Metadata and reference data management (MRDM)	The MRDM track alleviates challenges arising from different standards, definitions and reference codes by collecting information from disparate source systems and storing that information in a centralized repository.
Data architecture	The data architecture track ensures key Medicaid-focused data domains are identified, defined and managed appropriately within the HHS system.
Data and information controls (DIC)	The DIC track is responsible for the identification, definition, creation and implementation of various controls and metrics. It also identifies and monitors various data controls like data security and data access.

Texas HHS also partners with academic institutions, such as Dell Medical School to leverage expertise available to help expand HHS's ability to analyze data.

Health IT Topic: Identity Management, Provider Directories and Attribution

The ability to accurately and irrefutably identify the Medicaid community – both providers and members – is essential to ensuring the right services are delivered to the right individual at the right time. Denying an individual Medicaid services because of inaccurate information presents risks and unnecessary hardships to those the state is committed to protect. Additionally, the availability of location and contact information for Medicaid services providers is essential to all facets of care delivery.

The Texas HHS strategy to mitigate these risks is to make the best information easily accessible on member eligibility and provider locations on platforms and media used by Medicaid clients and healthcare providers.

Eligibility as a Service

Eligibility as a Service (EaaS) is a web service implemented at the Texas Medicaid claim administrator's, Texas Medicaid Healthcare Partnership (TMHP), website. This near real-time Medicaid eligibility service enables MCOs' and providers' systems to obtain access to a Medicaid member's current eligibility status. Access to eligibility information ensures MCOs' and providers' decisions are based on the most current eligibility information available. This minimizes the likelihood of a client being incorrectly denied services and assures providers reimbursement for the services provided to a client. The EaaS service is also interfaced with the TMHP client portal, TexMed Client Portal, which enables members to obtain access to their history and eligibility information in near real-time. Providers also use this portal to obtain access to clients' claims data, which is helpful when dentists or physicians are seeing patients for the first time and require relevant history prior to performing tests or procedures.

The EaaS web services uses the Texas Integrated Eligibility Redesign System data to produce the HIPAA compliant X12 standard-based client eligibility query and response electronic data interchange. HHS is using the near-real time accuracy of the data to incent its stakeholders to use the web services instead of older format, legacy eligibility information which is updated less frequently. To date, many of the high-volume users, including the behavioral health system used by many of the state's providers, have converted to the EaaS web service. HHS continues to work with its stakeholders as they adapt their systems to the EaaS format.

EaaS is also used by the HHS/DSHS Data Integration and Exchange Platform. Using EaaS, DSHS can identify the state laboratory's test results belonging to Medicaid-eligible clients. The results are sent to Medicaid and used to update the appropriate health information records.

Provider Directories

HHSC is in the process of implementing a Provider Management and Enrollment System (PMES) for provider enrollment and management. PMES is fully compliant with all state and federal laws, including but not limited to the Patient Protection and Affordable Care Act; 42 Code of Federal Regulations (CFR) 455; S.B. 200, 84th Texas Legislature, Regular Session, 2015, requiring the state to consolidate and streamline its provider enrollment and data management processes; the 2016-17 Texas General Appropriations Act (H.B. 1, 84th Legislature, Regular Session, Article II, HHSC, Rider 95); and S.B. 760, 84th Texas Legislature, Regular Session, 2015, regarding provider credentialing and monitoring.

The implementation of a PMES modernizes, streamlines, consolidates and advances the Provider Enrollment and Provider Management activities and supports electronic signatures and attachments. PMES is a cornerstone of the MMIS modernization process. The PMES solution replaces multiple paper and online enrollment applications with a single online application and provides the ability to manage,

correspond, track, monitor and report on all aspects of provider enrollment, disenrollment, re-enrollment, revalidation, inquiry and maintenance of Medicaid providers and any additional non-Medicaid providers currently within the scope of operations supported by the Medicaid program. The system will utilize the National Provider Identifier fully. Implementation includes an Online Provider Directory with information on HHSC Medicaid providers classified by type, specialties, credentials, demographics and service locations. The system is scalable and can be expanded to include attributes and information needed to support the management of providers across the HHS system in the future. Other features include:

- Lowers provider frustration by offering one place to enroll in all HHS programs;
- Improves the accuracy of provider location information and network adequacy metrics;
- Provides the capability to access comprehensive data needed to effectively monitor providers;
- Delivers a centralized provider repository that aligns with the ongoing data governance provider efforts and streamlines provider enrollment and management processes; and
- Secures efficient and effective business functionality and processes in support of Texas providers, clients and medical, dental and pharmacy benefit programs.

PMES will serve as the authoritative Medicaid provider information source for the master provider index under development by the Enterprise Data Governance project. Future PMES deployments will integrate the remaining HHS provider groups with the implementation of additional HHS program requirements.

Patient and Provider Master Indices

HHS currently has an IAPD with CMS to implement master data, metadata improvement and data quality controls. HHS has already implemented a Medicaid provider and member master data system to resolve identities across a variety of HHS systems.

As standards-based clinical data sources from provider EHRs are made available through the iCoE, these mastered records will be updated to assist in matching clinical records. Master records will also assist data analytics teams in creating connections to services data for ad hoc analytic uses. They are also foundational for development of future analytics architectures that could be capable of longitudinal views or aggregate groupings of the data (e.g. by care episodes or cohort types).

A Medicaid master provider record has been published for enterprise consumption in fiscal year 2019. These mastered records are easily extensible for use in managing clinical records as they arrive at HHS. A Medicaid master member record has also been implemented and is scheduled to be published for internal use in fiscal year 2020. These mastered records can also be extended for use as a master patient index to coordinate consumption of electronic health records or messages, as those become available to HHS.

Health IT Topic: Promoting and Funding Provider Health IT Adoption and Use

The Health IT adoption strategies build on Texas' Health IT ecosystem by increasing the number of connected Medicaid providers, expanding the HIE network and establishing a single state-designated connection point for the secure exchange of clinical data with Texas HHS, MCOs and national networks. It is critical to solidify a pathway that can be shared across the state and with Medicaid for the receipt of clinical data.

Medicaid MCO and Dental Contractor HIE Participation

In August 2016, HHSC polled the 19 Medicaid healthcare MCOs and two Medicaid dental contractors about their participation in health information exchange. With respect to health information exchange, 4 of the 19 healthcare MCOs, or 21 percent, indicated they exchanged member health information with a health information organization. Among the 79 percent who did not exchange member health information, several gave reasons including concerns over privacy and HIPAA compliance. Other responses included that the MCO lacked exchange access in their service area or that the limited functionality of the exchange in their service area did not warrant participation.

Seven of the 19 healthcare MCOs, or 37 percent, responded that they or their network providers receive or share patient encounter alerts or the raw HL7 ADT messages upon which these are based. Five of the 19 healthcare MCOs, or 26 percent, indicated their network providers receive alerts after patients are admitted to hospital emergency departments.

The two dental contractors did not participate in HIEs.

DSRIP Provider Health IT Adoption and Use

As part of DSRIP semi-annual reporting in 2017, DSRIP providers were required to respond to questions relating to the extent to which they participated in health information exchange with other providers and organizations, the types of information shared and factors impacting their participation. Of the 297 DSRIP providers, about 55.6 percent indicated they exchanged data, such as claims and clinical information, related to their DSRIP projects. However, about 17 percent of all DSRIP providers indicated that they did manual data exchange (e.g., fax and email). Only 22.6 percent of DSRIP providers indicated they participated in a formal HIE related to their DSRIP projects. Of those, 56.7 percent participated in one of the public, Local HIEs. The remaining 43.3 percent either participated in a private (e.g., hospital system HIE) or an interoperable vendor HIE that allows all providers using the same EHR vendor platform to exchange information.

The most common obstacle the providers identified to participating in the exchange of health-related information was lack of technology. Many of the providers operate in the “white space” where no HIE is available. The second most common obstacle was the cost of technology. Additionally, several providers indicated there were “other” barriers, with the most common “other” challenge being a lack of compatibility and interoperability across HIE systems.

Medicaid Electronic Health Record Incentive / Promoting Interoperability (PI) Program

In Texas, EHR use has climbed to rates close to those of national levels. The Texas Medical Association reports that over 85 percent of physicians are using EHRs in their daily practice.[5]

Texas’ Medicaid EHR Incentive/PI Program is a federal program administered by HHSC which provides incentives to Medicaid eligible professionals and eligible hospitals. The incentive payments, via 100

[5] Texas Medical Association 2018 Survey of Texas Physicians: Research Findings. Accessed September 26, 2019 at: https://www.texmed.org/uploadedFiles/Current/2016_Advocacy/2018_Final_Survey_Report_v2_3_14_19.et_FINAL.pdf

percent federal funds, are provided for the adoption and subsequent meaningful use of CEHRT. Providers report on PI/meaningful use and clinical quality measures established by CMS.

Texas' EHR Incentive/PI Program has provided almost 11,000 Medicaid providers with financial resources to implement electronic systems. Projected outcomes include:

- More accurate and complete information about a client's health, which allows them to deliver more quality care;
- Decreases in fragmented care across care coordination teams, which is important for managing chronic and serious medical conditions;
- Secure information sharing with clients electronically, allowing for more client engagement in decisions regarding their health; and
- Timely information to help diagnose health problems sooner, reduce medical errors and provide safer care at potentially lower costs.

As of September 1, 2019, the program had disbursed over $864 million federal incentive dollars to 10,472 eligible Medicaid professionals and 343 hospitals. Texas providers have attested to 200 different CEHRT products. The top 20 CEHRT products nationwide are used by 77 percent of Texas program participants.

Eligible Professionals and Eligible Hospitals Achieving Meaningful Use Stage 1 (MU1) and Incentives Paid as of September 1, 2019

	Provider Count	Provider Count Achieving MU1	MU1 Achievement Percent	Incentives Paid
Eligible Professional	10,472	5,160	49.3%	$332,554,171
Eligible Hospital	343	313	90.5%	$532,081,350
Total Incentives Paid				$864,635,521

HIE IAPD Strategy 1: Medicaid Provider HIE Connectivity

HIE IAPD Strategy 1 is intended to assist Local HIEs with connecting to ambulatory providers and hospitals in their respective areas, including by reimbursing Local HIEs for connectivity costs incurred during the connection process. This strategy will build the critical mass of connected providers needed to create meaningful exchange of clinical data across Texas.

This HIE Connectivity strategy enables Local HIEs to transmit data through a set of state-level shared services made available to each local network by the Texas HIE platform. This model enables electronic exchange of clinical data among providers as well as with Texas Medicaid for better care coordination benefiting Medicaid patients.

HHSC recently concluded an open enrollment process to solicit Local HIEs for participation in this program. These activities continue through federal fiscal year (FFY) 2021. Funding allocated to Local HIEs through the enrollment process is a deliverable-based model, with the deliverables demonstrating

connections result in active transfer of CDA-based[6] or ADT-based clinical data to state Medicaid and between Medicaid providers.

Funds are targeted toward offsetting the cost HIEs absorb when establishing new connectivity for providers, are paid on a per provider basis and are based upon the type of connectivity for which a Local HIE requests reimbursement. Providers are responsible for their ongoing costs.

Responses to the open enrollment will include each HIE's average cost of connecting providers and hospitals to their HIE for the purposes of this program. Costs provided by the Local HIEs must be approved by HHSC prior to awarding contracts for connectivity implementation. Local HIEs must demonstrate the costs presented are comparable to their existing connectivity cost model and are aligned with current industry norms.

HIEs must demonstrate their technical readiness to establish EHR connectivity, including the capability of delivering CDA Transition of Care (CDA ToC) documents to Medicaid and the capability of enabling query-based exchange of those Transition of Care documents across the network to other Medicaid providers.

HIEs accepted into this program conduct business with Texas Medicaid by submitting the Medicaid Practice Onboarding Form for each Medicaid provider the HIE proposes to connect. This onboarding form provides Medicaid with the ability to ensure the provider for which connectivity is being proposed meets the eligibility criteria of the program. The Onboarding Form provides assurance that the HIE has the capability to connect the provider in a manner that meets the technical standards and program timelines set forth for the program. To ease the burden of HIEs in financing the expenditures involved in connecting providers, HIEs may elect on the Onboarding Form to apply for up-front payment of 20 percent of the approved cost of connecting the provider. HIEs will invoice HHSC per connection.

Incenting Provider HIE Participation through Low-Cost Connection Model

Texas HIEs are working to address the barriers faced by all levels of providers in connecting to the Health IT ecosystem. In El Paso, the Paso Del Norte Health Information Exchange (PHIX) is working one-on-one with providers to get their CEHRT connected. El Paso has many veterans whose visits to the U.S. Department of Veterans Affairs (VA) require them to provide their health histories. If PHIX HIE was connected to their PCP, this information could be provided to the VA using a database query. Without these connections, veterans are required to bring a paper copy of their health histories.

With PHIX's HIE vendor, each new connection required significant upfront costs for both the provider and HIE, as well as significant ongoing costs for providers. This is especially true for small practices. PHIX researched options for obtaining vendor integration services at more reasonable pricing. In 2018, PHIX concluded that using an open-sourced version of MIRTH to connect to the front-end of their HIE and using PHIX staff to solution the secure infrastructure and connectivity was the most economical approach. This solution, priced on a sliding scale based on the size of the practice, implements routine transmissions of standards-based clinical data C-CDA transactions to PHIX. To date, this solution has worked for three Federally Qualified Health Centers and one Local Mental Health Authority. Plans are in

[6] "CDA-based clinical record" is defined as the C-CDA Transition of Care document referenced in Promoting Interoperability and 2015 EHR Certification Final Rule published by CMS, conforming to the requirements and standards referenced at 45 CFR §170.315(b)(1)(iii)

the works to expand this solution to 10 additional provider locations with less than 5 physicians by January 2020.

This interoperable information exchange between healthcare providers serving the same veteran has improved services for patient, payer and provider with costs at a fraction of commercial prices. This approach is being shared among the HIEs in Texas as way to overcome the cost barrier.

Model for Data Exchange with Community-Based Providers

HHSC is applying for CMS' Maternal Opioid Misuse Model (MOM) grant program, which requires the ability to exchange EHRs across a participant's caregiver community that includes both Medicaid and non-Medicaid services. The HIE Connectivity Project, Strategy 1 of the HIE IAPD discussed in the prior section, provides the data exchange capabilities needed for Texas Medicaid to participate in innovative care models like the MOM program.

Community-based caregivers connected to a HIE can access and update patient records for services provided outside of the typical healthcare setting. The clinical data in combination with the claims and encounter data Medicaid already receives would enable data analytics teams to identify and assess member populations' healthcare costs and outcomes required for program oversight and reporting needs. This not only meets the requirements for the grant participation but serves as a model that can be extrapolated across the state.

Health IT Topic: Advancing the Use of Health IT to Support Quality Measurement

The ability of the Texas Medicaid Managed Care Program to transition to value-based payment and pursue meaningful healthcare quality improvement goals depends crucially on the availability of performance metrics that can reliably and consistently measure progress across all aspects of the program. These measures should leverage established data standards and consensus specifications to advance the aims endorsed by the National Academy of Medicine (formerly the Institutes of Medicine) in *Crossing the Quality Chasm*[7] that care should be safe, effective, patient-centered, timely, efficient and equitable. Within the Texas Medicaid managed care program, all major initiatives focused on improving quality and building value begin with data and center on measurement (see Appendix B for a description of the Texas Medicaid Value-Based Initiatives).

Despite this commitment to data driven decision-making, Texas Medicaid, like nearly all healthcare organizations, has opportunity for improvement. A recent review by the state's Value-Based Payment and Quality Improvement Advisory Committee, a multi-disciplinary panel of experts and healthcare industry leaders established by the Executive Commissioner of HHSC to help shape the direction of the APMs and other value-based initiatives in Medicaid, found that a significant amount of data is potentially available to support healthcare quality. This panel, however, found "that doesn't mean that HHSC, its contracted health plans and their network providers always have the information necessary to provide high-value, coordinated care. HHSC must have informative data –- both clinical and administrative -– to guide the program, and health plans and providers must have access to timely, trusted information as a foundation for engaging in value-based payment arrangements."[8] Ultimately, according to the advisory

[7] *Crossing the Quality Chasm: A New Health System for the 21st Century*. Institute of Medicine (US) Committee on Quality of Health Care in America. Washington (DC): National Academies Press (US); 2001.

[8] Texas Value Based Payment and Quality Improvement Advisory Committee (2018). *Recommendations to the 86th Texas Legislature: Opportunities to Advance Value-Based Payment in Texas.* Accessed July

committee, to fully implement effective value-based and quality improvement initiatives, the HHS System and Medicaid Program will need an informatics strategy that enables near real-time learning and incorporates both clinical and administrative data into robust measures of performance. These next generation informatics tools increasingly will guide decisions at every level, from state policy maker to clinician to individual patient.

To support this emerging emphasis on analytics, best practice and patient empowerment, HHS is working to bring analytics that include both clinical and administrative data to the forefront of healthcare quality measurement and improvement. Clinical data refers to the information derived from the medical interaction between a provider and a patient, including: medications, allergies, problem list, physical examination findings, laboratory and results from other diagnostic testing. Integrating this data with existing administrative or claims data submitted to document healthcare reimbursements promises to broaden the possibilities for successful value-based payment and quality improvement initiatives.

Over the past two decades, analytics based on administrative data have evolved to more reliably measure fidelity to recommended processes of care, i.e., whether a patient received appropriate services. However, in a value-based environment, measures used for decision making, quality improvement and payment must look beyond process to consider outcomes, the prevention and control of disease, as well as environmental and behavioral risks for poor health.

For example, as value-based payment and quality improvement systems become more advanced, indicators recommended by experts through organizations such as the National Quality Forum to identify high achievement in a field such as diabetes care generally look something like the following:

- A patient's most recent HbA1C in the measurement period has a value < 8.0;
- The most recent blood pressure in the measurement period has a systolic value of < 140 and a diastolic value <90; and
- The patient is currently a nonsmoker.

While claims are suitable for identifying a population of individuals with diabetes and some basic measures of quality, clinical and health risk data such as blood pressure control and tobacco use are needed to truly understand and improve the effectiveness of care delivery. Moreover, the near real time availability of electronically exchanged clinical data will significantly accelerate the time horizon for clinical and evaluative decision-making, expanding the possibilities for rapid-cycle improvement approaches.

Ultimately, individuals and the public will benefit from the timely computation, analysis and reporting of enhanced quality indicators based on combined clinical and administrative data because it paves the way to a more accountable, learning healthcare system.

HHSC began assessing payment methodologies between MCOs and providers beginning in 2012. These early reviews indicated that while MCOs received capitated premiums from HHSC and generally operated in a value-based environment, they still predominantly reimbursed providers using a fee-for-service approach, thus maintaining incentives for volume over value in the payment model.

To help promote transformation to a Medicaid system that rewards the achievement of good patient outcomes at lower cost, HHSC created contractual targets for MCOs to link a portion of provider

18, 2019 at: https://hhs.texas.gov/sites/default/files/documents/about-hhs/communications-events/meetings-events/vbpqi/jan-2019-vbpqi-agenda-item-6.pdf

payments to value using APMs starting in calendar year 2018. APMs are value-based contracting models where providers assume increased accountability for both quality and total cost of care. The term is often used synonymously with value-based payment (VBP) but may also refer to a more systematic approach to VBP where APMs exist along a continuum with progressively greater emphasis on the management of a population (e.g. shared savings, bundled payments and capitation). MCOs must meet targets both for overall value-based payment and for risk-based APMs. If an MCO fails to meet the APM targets or certain allowed exceptions for high performing plans, the MCO must submit a corrective action plan and HHSC may impose contractual remedies, including liquidated damages.

APM Contract Targets with Providers

Year	Overall Target	Risk Based Target
2018	25% of medical expense in a VBP model for MCOs and dental contractors (DCs)	10% of medical expense in a risk based VBP model for MCOs; 2% for DCs
2021	50% of medical expense in a VBP model for MCOs and DCs	25% of medical expense in a risk based VBP model for MCOs; 10% for DCs

The APM initiative, which aligns with the nationally recognized framework established by the Health Care Payment Learning and Action Network,[9] has already seen some initial progress at aligning payment with value. As of the beginning of 2018, even before the effective date of initial contractual targets, about 40 percent of MCO payments to providers for medical services has migrated to a value-based model.

Electronic clinical quality measures (eCQMs) help to measure and track the quality of healthcare services, based on data generated by a provider's EHR. The availability of clinical metrics will strengthen opportunities for MCOs and providers to adopt more powerful APMs that move closer to population-based payment. The state also sees potential for these measures to help reduce any administrative complexity associated with the changing payment model.

Administrative complexity lowers provider productivity, satisfaction and diverts energy and resources that otherwise could go toward improving patient care. The Value-Based Payment and Quality Improvement Advisory Committee plans to devote a significant portion of its upcoming work on ideas to harmonize VBP approaches, including by recommending common outcome measures for use in APMs. Standardized eCQMs will be considered as part of these deliberations and should support administrative simplification related to the APM initiative.

Federal and state law for Medicaid Managed Care require ongoing reporting on MCO performance, as well as continuous quality improvement. The electronic exchange of data and availability of robust clinical quality measures will invigorate these current efforts. The state's External Quality Review Organization (EQRO) routinely assesses quality, timeliness and access to healthcare for Texas Medicaid and CHIP

[9] Health Care Payment Learning & Action Network. *Alternative Payment Models (APM) Framework*. July 11, 2017. Accessed July 18, 2019 at: https://hcp-lan.org/apm-refresh-white-paper/

recipients.[10] Metrics reported by the EQRO are used for several critical purposes to promote quality improvement and value, including the development of report card ratings for individual health plans. In addition, the EQRO plays a central role in facilitating MCO Performance Improvement Projects (PIPs). Each health plan is required to conduct two, two-year PIPs per Medicaid program.

At least one of these projects must be collaborative, involving another MCO, DSRIP providers and/or community-based organizations. PIPs typically follow a recognizable quality improvement (QI) cycle encompassing root cause analysis, baseline measurement, intervention, remeasurement and assessment.

Recent projects have covered priority QI topics such as improving control of asthma and high blood pressure and reducing potentially preventable hospital and emergency department admissions, all areas that intersect with eCQMs.

Health IT Topic: Health IT and Service Delivery

Health IT presents the opportunity to improve service delivery through a variety of mechanisms. It is a major tool to facilitate improved coordination and integration between Medicaid providers, including physical health, behavioral health and home-and community-based services providers. Obtaining measurable, actionable data is at the heart of value-based care models. Quantitative and qualitative data analysis to assess performance against meaningful outcome measures identifies where the health system can deliver value. Further, tools such as telehealth and telemedicine are critical in supporting health system goals, such as achieving provider network adequacy in Texas' vast rural regions.

Care Coordination under the Managed Care Delivery System

To address their care needs comprehensively, patients often require multiple touchpoints within a single provider's care team or must be seen by multiple provider types across the spectrum of physical health, behavioral health and home- and community-based services providers. Further, as the complexity of a patient's needs increases, so does the potential for medical errors, duplication of services and unnecessary tests. To compound this complexity, the ability of a patient to achieve optimal health outcomes may be intertwined with medically relevant non-clinical factors, such as access to adequate housing, transportation and social supports.

One of the promises of Medicaid managed care both in Texas and across the nation is to optimize care coordination. The long-term pathway to the most effective care coordination would include providers using EHR technology to integrate all relevant patient care information and distribute that information effectively among authorized providers.[11]

Findings of a study directed by the 2018-19 Texas General Appropriations Act,[12] which required that HHSC conduct a review of the agency's contract management and oversight for Medicaid managed care contracts, further supports the role of Health IT in care coordination. The Rider 61 report acknowledged that the HIE Connectivity Project was introduced with "the primary objectives of advancing care

---

[10] Institute for Child Health Policy (2018). *Summary of Activities and Value-Added Services State Fiscal Year 2018: Quality, Timeliness, and Access to Health Care for Texas Medicaid and CHIP Recipients*. Accessed July 18, 2019 at: https://hhs.texas.gov/sites/default/files/documents/laws-regulations/reports-presentations/2019/egro-summary-of-activites-report-contract-yr-2018.pdf

[11] https://www.healthit.gov/topic/health-it-basics/improve-care-coordination

[12] S.B. 1, 85th Legislature, Regular Session, Article II, HHSC, Rider 61(b)

coordination through increased HIE adoption and use by Texas Medicaid providers and creating additional capacity in Texas that can support that use and adoption."[13]

Because of Rider 61, HHSC developed several focused initiatives for improving Medicaid managed care oversight, including an initiative to make improvements related to service and care coordination within managed care. HHSC's Managed Care Oversight Improvement Initiative related to care coordination and service management intends to:

- analyze other state Medicaid programs to assess best practices for care coordination within Texas' managed care programs;
- address any state-level barriers that hinder MCO delivery of care coordination services;
- simplify terminology and clarify definitions of service coordination and service management activities across product lines; and
- identify possible improvements to ensure service coordination and service management is consistent within HHSC contract requirements.

Within these initiatives is the opportunity to assess how Health IT and HIE can overcome barriers to care coordination and service management and identify opportunities for improvement in the contract requirements within Texas' Medicaid managed care models. For example, there could be an assessment of the clinical information exchanged between HHSC, MCOs and Medicaid providers and requirements for how information is conveyed from MCOs to their staff who serve care coordination functions.

Medicaid MCO and Dental Contractor (DC) Portals

MCO and DC portals present the opportunity to empower providers with information to effectively coordinate member care and members with the information to understand their health and better advocate for their needs.

In August 2016, HHSC polled the 19 Medicaid healthcare MCOs and two Medicaid dental contractors about their portal capacity. MCOs were asked about the data that network providers could access as well as the types of data that MCO members could access. More MCOs made health data about members available to network providers than to the MCO members themselves. Only 8 of the 19 MCOs made data about the primary categories of health data about which the MCOs were polled (claims-based data, prescription history and clinical data) available to MCO members. These portal poll results follow:

Information Accessible to MCO Network Providers about their Clients via MCO Portal

Response	Claims-based Data (e.g., diagnosis and procedures)	Prescription History	Clinical Data (e.g., lab results and immunizations)
Yes	84%	32%	32%
No	16%	68%	68%

[13] HHSC. *Rider 61: Evaluation of Medicaid and CHIP Managed Care,* August 17, 2018. Accessed July 18, 2019 at: https://hhs.texas.gov/sites/default/files/documents/laws-regulations/reports-presentations/2018/sb1-rider61-evaluation-medicaid-chip-august-2018.pdf

Information Accessible to MCO Members about their Health Data via MCO Portal

Response	Claims-based Data (e.g., diagnosis and procedures)	Prescription History	Clinical Data (e.g., lab results and immunizations)
Yes	11%	42%	16%
No	32%	0%	26%
N/A	58%	58%	58%

Both DCs had a portal that enabled network providers to see their clients' claims-based data, but not prescription history or clinical data. Also, neither of the DCs had a member portal that shared health data as of August 2016, though one of the DCs indicated they were about to launch their member portal that would enable members to view their claims, including which procedures they had.

Advances in the sophistication of MCO and DC portals has occurred since 2016, presenting an opportunity to reassess current portal capabilities and identify if any improvements could be made to portal-related managed care contract requirements.

Health IT in DSRIP

Many of the most transformative types of DSRIP projects, including integrating physical and behavioral healthcare, patient-centered medical homes, chronic care management and patient care navigation, fundamentally benefit from the timely exchange of accurate health data. DSRIP has incentivized providers to implement Health IT tools and build local data-sharing relationships that enhance care transitions, care coordination and health system navigation. Further, DSRIP has motivated providers to build internal Health IT infrastructure as well as connect to external data sources to elevate data-driven decision-making, conduct more meaningful performance measurement and engage in continuous quality improvement. Finding ways to sustain and expand upon the successful use of Health IT in DSRIP is a critical component of DSRIP transition planning for when program funding ends October 1, 2021.

Emergency Department Encounter Notification System

HHSC's EDEN system, discussed in greater detail in this plan's Health IT Ecosystem section, implements a major tool for handling care transitions with the transmission of ADT information to MCOs, providers and the state. This is the first step in Texas Medicaid's use of clinical data to facilitate care coordination. EDEN is implemented utilizing push technology which is recognized as the preferred method for sending electronic notifications. Push technology is a recently added exchange modality in the TEFCA proposed by the ONC.

Telemedicine/Telehealth

Telemedicine and telehealth are part of the larger Texas strategy to deliver services in a more efficient, innovative way and enhances network adequacy, including in rural areas. Telemedicine services are defined in Texas law as healthcare services delivered remotely to a patient by a physician, or other healthcare professional under physician delegation and supervision.

It has the potential to offer convenient access to routine care for Medicaid clients who might otherwise be unable to receive in-person services. Using telemedicine, physicians and other healthcare providers can receive supervision and guidance on patient care from specialty-care physicians. Telemedicine can improve both the access and quality of care.

Telehealth services are defined in state law as healthcare services delivered remotely to a patient by a healthcare practitioner who does not deliver telemedicine services. In practice, this means that telehealth services are non-physician delivered services. Licensed professionals such as counselors, midwives and dieticians can deliver telehealth services.

The number of Texas Medicaid clients using telemedicine and telehealth services grew 30 percent from fiscal year 2016 to fiscal year 2017. The number of providers offering these services increased 32 percent during that same period. Texas Medicaid's spending on telemedicine, telehealth and telemonitoring services nearly doubled, from $9.6 million in fiscal year 2016 to $18.4 million in fiscal year 2017. The spending increase is primarily due to a significant uptick in the use of home telemonitoring services. Home telemonitoring services, also referred to as remote patient monitoring, are the scheduled review of a client's transmitted clinical data. Types of clinical data include blood pressure and blood glucose measurements.

Telemedicine and Network Adequacy. State and federal laws require that MCOs meet travel time and distance standards, which measure access to care on a quarterly basis for 35 provider types in all 254 counties in the state. Medicaid is developing a methodology for counting telemedicine and telehealth services toward meeting travel time and distance standards.

Telemedicine in Rural Areas. Texas' strategy to address rural healthcare shortages includes telemedicine. Among Texas' 254 counties, 189 counties, in mostly rural areas, are at least partially designated as a primary care Health Professionals Shortage Area (HPSA).[14] Finding efficient, patient-centered approaches to deliver high-quality healthcare services to underserved rural regions is a critical issue for Texas. Telemedicine programs can enhance the viability of rural hospitals through the provision of specialized medical services.

Over the course of several legislative sessions, Texas has been expanding the options for Texas providers to engage in telemedicine in ways that address access concerns in rural areas. For example, in 2017, the Texas legislature created a new pediatric tele-connectivity grant program to provide funding to nonurban healthcare facilities to obtain telemedicine services from pediatric specialist physicians (H.B. 1697, 85th Legislature, Regular Session, 2017). The grant program will enable facilities that lack advanced neonatal intensive care unit capabilities to make appropriate and rapid medical decisions for the care of their newborns. In 2019, the Texas legislature passed legislation enabling satisfaction of physician requirements for Level IV trauma facility designation in counties with populations less than 30,000 using telemedicine (H.B. 871, 86th Legislature, Regular Session, 2019). Also, in 2019, legislation was passed to further broaden the array of Medicaid services available for telemedicine reimbursement under Medicaid managed care (S.B. 670, 86th Legislature, Regular Session, 2019).

HIE and Emergency Medical Services

Texas HIEs have also explored methods for enhancing service delivery. The Harlingen, Texas based Trauma Regional Advisory Council asked their HIE, the Rio Grande Valley Health Information Exchange

[14] Health Resources & Services Administration. Health Professional Shortage Areas (HPSAs). https://bhw.hrsa.gov/shortage-designation/hpsas

(RGVHIE), to identify a method for improving communications between EMS 911 providers (EMS) and hospital EDs. RGVHIE developed three approaches for improving communications:

1. **EMS Data-hub.** The EMS Hub integrates with a wide range of EMS Electronic Patient Care Reporting (ePCR) software serving as a conduit for health information exchange by storing "run reports" and making them available via a Provider Portal. Run Reports are required from an EMS organization within 12-24 hours after a patient is delivered to an emergency room. Run reports were typically delivered via fax or paper. The process was fraught with inefficiencies and timeliness issues. Hospital and EMS personnel now have real-time access to run reports stored in the EMS data hub using the HIE-based web portal.
2. **EMS App and Hospital Notifications System.** This service allows for EMS to send a pre-notification alert to a receiving hospital about an individual's status directly onto a dashboard in the Hospital Emergency Department to provide decision support and prepare for an individual's arrival—especially for conditions requiring time-sensitive treatment or therapy—such as trauma, heart attack or stroke. The EMS App is a tool for paramedics on the field responding to 911 emergency calls to capture patient information and send real time to Hospital Emergency Room personnel.
3. **EMS access to real time patient information at the point of care.** There was consensus across RGVHIE EMS stakeholders that access to patient information would be beneficial at the point of care. Since most of the ePCRs did not have integration capabilities, RGVHIE initially solutioned this with an EMS app external to the EMS workflow. There was minimal participation and difficulty with the patient identification process. RGVHIE is continuing to work through these challenges and others.

RGVHIE learned that while it is beneficial to have maximum patient information available, the system must account for workflow adoption and variations in infrastructure standards. RGVHIE surveyed their customers and had a 77 percent response rate. A resounding 80.5 percent of respondents indicated it is extremely useful for them to be able to retrieve patient information from other hospitals, EDs and physician practices through HIE. One hundred percent of participants noted that the most important function of HIE will be obtaining mental health diagnoses and pathology reports.

Disaster Response - PULSE

PULSE is a nationwide Health IT disaster response platform that can be deployed at the city, county or state level to authenticate and assist disaster healthcare volunteer providers.

PULSE allows disaster workers to query and view patient documents from all connected healthcare organizations. To ensure the maximum amount of medical information is electronically available about Texans during a disaster, HHSC is proposing to implement PULSE in partnership with THSA. In 2017, the THSA's query-based HIE services were scheduled to terminate as THSA was in the process of converting HIETexas, the THSA's state-level HIE network, from query-based exchange services to an alerts-based care coordination platform. However, THSA delayed that transition after Hurricane Harvey hit Texas and there was a need to continue offering query-based HIE to assist in the recovery efforts by allowing patients' health information to follow them.

During the response to Hurricane Harvey, Texas HIEs set up access in select shelters and provided patient look-up services to medical teams operating in those environments. Although several successful information hits resulted, the process needs to be scaled and standardized across the state.

PULSE, initially developed by the State of California with ONC grant funding (2015-2017), is a non-proprietary, open-source software solution operated for California by Audacious Inquiry (Maryland) and hosted by The Sequoia Project. PULSE was designed to be expandable to all parts of the United States.

PULSE represents a significant improvement over the HIE involvement during the Hurricane Harvey response. It provides emergency healthcare workers direct access to broader sources of critical health information. Texas is proposing to implement PULSE through IAPD funding requested to leverage and expand the state-level services, HIE and provider connectivity included in all the strategies of the previous IAPD.

During disasters, Texas' large and highly complex healthcare delivery system performs as a health information exchange model with HIEs that have limited interoperability across the state. An interoperable model is required to support meaningful coordination of care as services are delivered in shelter sites. It is essential that the most clinically relevant information be available to support individuals involved in disaster situations. The access and use of health information is critical to patient quality of care during these times of crisis.

The project is based on a use case that incorporates interoperable health information technology tools and services that support disaster response activities in shelter locations. It will incorporate national standards that facilitate health information exchange and build upon the HIE work already accomplished in Texas.

Behavioral Health

Behavioral health has been a priority focus for Texas over the last several years as demonstrated through significant policy-making, strategic planning and legislative funding commitments. Texas Medicaid and CHIP has been working on several initiatives to improve outcomes and reduce costs for providing services to individuals with Behavioral Health (BH) diagnoses. The capacity for providers to coordinate care through the sharing of health information will help Texas Medicaid achieve these initiatives, which are as follows:

- Implementation of federal and state mental health parity standards, which require that individuals do not experience more barriers accessing mental health and substance use disorder services than they do accessing medical and surgical services;
- The creation of managed care requirements around integrating behavioral and physical healthcare at the MCO and provider levels;
- Evaluation of a pilot program studying integrated behavioral and physical healthcare led by behavioral health clinics and including the implementation of alternative payment methodologies in integrated care clinics;
- Implementation of a peer support benefit for individuals with mental health and substance use disorder conditions; and
- Improving access to medication assisted therapy and other evidence-based treatments for substance use disorders.

The Health IT approach to behavioral health cross-cuts many Health IT topics, which necessitates the comprehensive discussion that follows.

Prevalence of BH diagnoses in Texas Medicaid

More than 290,000 Texas Medicaid and CHIP clients had a diagnosed serious emotional disturbance (SED) or serious mental illness (SMI) in state fiscal year 2016. The most common SED/SMI diagnoses are major depression, schizophrenia and bipolar disorder. A much larger number of clients experience mental health conditions that do not rise to the level of a SED/SMI but do impact daily life, such as anxiety disorders. Still others have diagnosed substance use disorders, such as opioid use disorder or alcoholism.

Health IT's potential for physical and behavioral health integration

Care coordination across physical and behavioral health is of sentinel importance to ensuring good outcomes. Behavioral health conditions are associated with significant physical comorbidities, which can increase the cost of care and result in poor health outcomes. Individuals with mental illness are also more likely to develop chronic medical conditions and become physically debilitated earlier in life, increasing acute and long-term costs. Behavioral health conditions are associated with 22 percent of Texas Medicaid managed care potentially preventable admissions and 46 percent of potentially preventable readmissions. Almost 66 percent of Texas Medicaid clients with three or more ED visits and two or more admissions in a year have a chronic behavioral health condition. According to a national study, significant numbers of nursing facility residents had a primary diagnosis of mental illness, with 25 percent being younger than age 65. Some medications required to manage the symptoms of serious mental illness can increase the risk of chronic physical conditions, such as metabolic disorders (e.g., diabetes).

When health information, such as medical history, lab results, medication lists and treatment plans for physical and behavioral health is not electronically exchanged, providers may prescribe treatment that compromises the person's safety, disrupts their recovery, or otherwise negatively affects their overall well-being. In cases where people with more severe conditions must see multiple providers, the risk that they will receive fragmented and inconsistent episodic care increases (e.g., people with depression are three times more likely to be noncompliant with their medical treatment regimens), which contributes to a shorter life expectancy.

The ability for behavioral and physical health providers to electronically share data on conditions and treatments enhances coordination of care, reduces/prevents adverse health events and improves outcomes of care.

Without connectivity to the Health IT ecosystem, the state must rely on its medical benefits claims processing system (Compass21) and outpatient pharmacy claims processing system (OS+, which is managed by Conduent) to manage whole-person care in individuals with behavioral health conditions. These systems are not connected and, as an example: a client could receive the buprenorphine implant (J0570) in a physician's office or outpatient hospital as a medical benefit (Compass21) and also receive an outpatient prescription by a different provider (i.e., pharmacy claims processed by OS+) that would interact negatively with the buprenorphine without either provider being aware, which could result in serious complications for the client.

Behavioral health providers have been working to use EHRs. This has been an issue for both behavioral and physical health providers who are working to integrate care within their practice, as many EHRs are not built to accommodate the needs of an integrated provider and require technical modifications. In addition, behavioral health providers are beginning to enter APMs with some MCOs, which often require EHR modification for quality measure data. These types of modifications can assist providers in addressing the needs of individuals with co-occurring conditions, but can be expensive and cost prohibitive. Assistance to providers will be necessary to support advances in an integrated care model.

HHSC maintains an electronic data system known as Clinical Management for Behavioral Health Services (CMBHS). CMBHS serves as an EHR for contracted providers of substance use disorder (SUD) services, and it serves as a data reporting system for contracted providers of mental health services.

For SUD services, CMBHS captures clinical documentation at a detailed level, including such things as client profile, screening, assessment, service type, treatment, progress notes, lab results, medication administration and service authorization. CMBHS also supports submitting claims to TMHP both for block-grant-funded SUD services and for a limited set of Medicaid-funded SUD services. Entering data for SUD services is currently only supported through a web-based interface in which providers directly enter the data. SUD providers who maintain their own electronic health record have the option of exporting their data, so it may be imported into their local systems.

For mental health services, CMBHS primarily serves as a data reporting system. It captures client profile, diagnosis, assessment, service authorization and it supports submitting claims to TMHP for certain Medicaid mental health programs. The system is primarily used by the Local Mental Health Authorities (LMHAs) and by other Medicaid providers of mental health case management and mental health rehabilitation services. Data for mental health services may be entered directly through the web interface, but LMHAs, with their own electronic health records, may submit information through an electronic data exchange.

Although CMBHS supports a variety of nationally-recognized vocabulary standards including the Diagnostic and Statistical Manual, ICD-10, and the National Drug Code, at the time of development there were no available national data standards that sufficiently addressed the medical and care delivery needs for patients with serious mental illness. This was recognized by HL7, which, at the time, had a workgroup on community-based collaborative care. To enable the LMHAs to extract data from their local EHRs and submit it electronically to CMBHS, the state worked with the primary EHR vendors of the LMHAs (Cerner, iServe, & Netsmart) as well as IT directors from the LMHAs to develop a set of standards and data definitions which are still in use today. All 39 of the LMHAs in Texas engage in some form of data exchange with CMHBS; but 35 of them utilize all the data exchange functions. The other four use a combination of data exchange and direct entry.

CMBHS is planned to be the system of record for commitment information, which is currently captured in various systems. Outpatient community center commitments are captured in CMBHS. State hospital commitments are captured in the Avatar systems maintained by the state hospitals, but it is also transmitted to the legacy mental health system, known as CARE. Current plans are to migrate remaining CARE functions to CMBHS when funding becomes available.

CMBHS could play an effective role in integrating behavioral health services into a care coordination system, but not without enhancements to its data exchange process. As CMBHS currently only supports the exchange of behavioral health data using custom interfaces, further development work would be required to make CMBHS compliant with ONC proposed national standard for USCDI and to meet the HL7 C-CDA standards. Making these enhancements in CMBHS and having our contracted users make the same enhancements to their local systems would allow CMBHS to be interoperable, exchange behavioral health data and receive other forms of health data in a meaningful way.

The state's and MCOs' ability to effectively manage the Medicaid system to achieve good outcomes for Medicaid and CHIP members with behavioral health conditions can also be enabled through improvements, standardization and connectivity to the Health IT ecosystem.

Connection of BH provider EHRs and CMBHS

Once behavioral health provider EHRs and CMBHS are connected to the Health IT ecosystem, MCOs and state staff would be able to access clinical data on member characteristics that would aid in the identification of specific needs. These denotations include certain behavioral health diagnoses for whom MCOs are contractually required to provide high levels of care coordination, and members enrollment in specific waiver programs with whom MCOs are contractually required to coordinate in creating service plans and authorizing medically necessary services. This information could also assist the state in data analysis to identify common diagnoses on which policies or programs to improve outcomes may be focused, and to ensure that members are not enrolled in more than one waiver program at a time.

Connectivity to provider EHRs would also enable access to information on court-ordered psychiatric services and would assist MCOs and the state to ensure that all court-ordered services are delivered and reimbursed, and that members who have been court-ordered into services get needed supports as court orders expire to prevent further criminal justice involvement and reduce emergency department use and hospitalizations.

As non-medical clinically necessary information is integrated into CEHRT, provider EHRs would also indicate when a member is experiencing a non-healthcare need that impacts health, such as housing instability or interaction with the criminal justice system. This would allow MCOs to identify members with further care coordination needs and would allow the state to work with other state-level systems such as the Texas Department of Housing & Community Affairs and the Texas Commission on Jail Standards to coordinate needs of Medicaid and CHIP participants.

Goals/Milestones

While this Health IT Strategic Plan details many important initiatives that advance Health IT, the milestones described in the table that follows represent core activities to services and providers across the continuum of care. HHSC considers this plan a living document that may be adapted to meet evolving needs.

Health IT/ HIE Strategy	Service or Application	Measure	FFY 2020/2021 Milestones
HIE IAPD Strategy 1	**Connections**	Number of Medicaid providers connected to Local HIEs by this project, with capability to transfer C-CDA or ADT-based clinical data	Goal is two hundred (200) Medicaid providers connected to Local HIEs as an outcome of this project
HIE IAPD Strategy 2	**Onboarding Local HIEs to THSA**	Number of HIEs connected to the THSA by this project	Goal is eight (8) HIEs connected to THSA as an outcome of this project
HIE IAPD Strategy 2	**Master Patient Index**	Implementation of Master Patient Index	Master Patient Index implemented

Health IT/ HIE Strategy	Service or Application	Measure	FFY 2020/2021 Milestones
HIE IAPD Strategy 3	**Medicaid Emergency Department Encounter Notification**	Number of HIEs contributing hospital emergency department ADT data	Goal is eight (8) HIEs contributing hospital emergency department ADT data as an outcome of this project
Initiative	**PULSE**	Program Planning and Implementation	Develop Plan and PULSE Application. Test and Launch PULSE Application and Implement Program

Conclusion

The primary objectives of this Health IT Strategic Plan are to establish a Health IT or HIE model that achieves better health outcomes for Texas Medicaid clients and to bring increased value to healthcare providers, institutions and community partners to best serve the Texas Medicaid population. Our intent is to develop a pragmatic, achievable and meaningful strategy that motivates state agencies and healthcare providers to adopt interoperability and Health IT infrastructure in support of achieving better health outcomes for the people we serve. Meaningful health data collection strengthens understanding of the relationship between social determinants of health and healthcare use across diverse populations, allowing the state to develop solutions to better connect patients to much needed services.

Propagating the transmission of ED ADT data will demonstrate the value to PCPs and healthcare providers of participating in data exchange. This is a first step in the use of clinical data for care coordination, but we must take subsequent steps beyond ED data notifications. Push technology is one way of exchanging information, but not the only one and not for all use cases. The ability to ask for information that is needed for care is another widely used method to support APMs. This Health IT Strategic Plan demonstrates an initial pathway, but Texas must also scale the solution beyond ED data to enabling push notifications between healthcare providers and payers. True care coordination will happen with information exchange among all care providers on the care team throughout the care continuum.

Not all healthcare providers and Medicaid payers will swiftly adopt the idea of connecting to HIEs to transmit data to other providers, other HIEs or state HHS entities. Many of the reasons for this reluctance are described in this plan. Large hospitals, provider groups and MCOs may recognize the most value in client data transmission and with their more robust resources are likely to adopt and implement HIE. However, it is unrealistic to expect 100 percent adoption from the healthcare community. Rural providers and practices that treat a small population of patients are likely be the last to adopt HIE; because, they are the most resource constrained.

Texas HHS must diligently work directly with HIE networks, THSA, provider associations, healthcare providers and MCOs to communicate the HIE value proposition and assist with bringing value to their respective organizations. Every organization strives to improve health outcomes for their patients, but how to achieve this vastly differs among organizations as the approach is governed by entity-specific priorities. Over the last five years, providers have encountered great expense and dedicated a significant amount of resources toward adopting and implementing EHR technologies. Their primary purpose is to provide high-quality services to the patients they serve, and Texas HHS can play a significant role in shaping a Health IT landscape that advances this objective.

The buildout of Health IT and HIE infrastructure is a critical component of furthering Texas HHS' vision of "Making a difference in the lives of the people we serve" and the mission of "Improving the health, safety and well-being of Texans with good stewardship of public resources."

Appendix A – Timeline of Health IT Legislation in Texas

Legislative action has been a significant driver for the advancement of Health IT in Texas. In 2005, the Texas Legislature created a multi-agency Texas Health Care Policy Council (Council) that was charged, among other directives, with "promoting the use of technology in health care to decrease administrative costs and to increase and improve the quality of health care."[15] In 2006, Governor Rick Perry established the Texas Health Care System Integrity Partnership, which recommended mechanisms for operationalizing the state-level recommendations of the Council.

In 2007, the Texas Legislature enacted Chapter 182 of the Health and Safety Code, which established the THSA. THSA is "a public-private collaborative to implement the state-level health information technology functions" and is intended to serve "as a catalyst for the development of a seamless electronic health information infrastructure to support the healthcare system in the state and to improve patient safety and quality of care."[16]

HHS agencies serve as ex officio representatives on the THSA board of directors. Texas HHS agencies work with THSA, HIEs and other stakeholders to advance the use of standards to support interoperability. Currently, the THSA is focused on:

1) expanding connectivity;
2) emergency department notifications;
3) support for statewide disaster response; and
4) public health reporting.

The Electronic Health Information Exchange System Advisory Committee was established to advise HHSC on issues regarding the development and implementation of the electronic health information exchange system in accordance with H.B. 1218, 81st Legislature, Regular Session, 2009. The committee was chaired by a member of the healthcare provider community and offered valuable stakeholder insight regarding HHS Health IT and HIE activities.

In 2010, HHS established the OeHC to serve as a single point of contact in HHS for health policy information, coordinate state level activities with THSA and serve as the State Health IT Coordinator and the central Health IT coordinator within the Texas HHS agency system.

In 2015, S.B. 200 removed over 20 advisory committees from statute, including the Electronic Health Information Exchange System Advisory Committee, and HHSC subsequently created the eHAC to advise HHS agencies on strategic planning, policy, rules and services related to the use of Health IT, health information exchange systems, telemedicine, telehealth and telemonitoring services.

H.B. 2641, 84th Legislature, Regular Session, 2015 required that information systems planned or procured on or after September 1, 2015 and used by a Texas Health and Human Services Agency to send or receive protected health information to and from healthcare providers use applicable standards and be interoperable with each other. H.B. 2641 aligns with federal legislation and promotes the use of certified electronic health record technology as well as requires information systems to follow the ONC's ISA.

[15] House Bill 916, 79th Legislature, Regular Session, 2005
[16] House Bill 1066, 80th Legislature, Regular Session, 2007

Appendix B – Texas Medicaid Value-Based Initiatives

Initiative	Description	Quality and/or Efficiency Measures	Benefit from Improved Health IT/HIE
Transition from Fee-for-Service to Managed Care	Over 90 percent of Medicaid and CHIP clients receive services through risk bearing MCOs and DCs. The transition to managed care has occurred in carefully planned stages over a 24-year period.	Federal and state law require several quality related activities including routine reporting on evidence-based measures of MCO and DC performance.	Care coordination is a foundation of the MCO service delivery model. The state's Health IT strategy will establish a reliable pathway for the expeditious exchange of high-quality data with MCOs and across providers engaged in the care of an individual. The availability of clinical data will also improve the relevance of program performance measures, including eCQMs.
MCO Pay for Quality (P4Q)	Budget neutral program that creates incentives and disincentives for MCOs and DCs. Health plans that excel on specified quality metrics are eligible for additional funds above their existing premium payments; health plans that do not meet their measures can lose funds.	P4Q includes industry recognized process and outcome measures within a model that: 1) is easy to understand; 2) allows health plans to track performance and improvement; 3) rewards both high performance and improvement; and 4) promotes transformation and innovation.	Improved HIE will allow for more timely assessment of MCO performance using the most meaningful metrics possible, including metrics showing clinical outcomes and that are appropriately adjusted for clinical and social risk.

Initiative	Description	Quality and/or Efficiency Measures	Benefit from Improved Health IT/HIE
Hospital Quality Based Payment Program for Potentially Preventable Readmissions and Complications	Provides incentives and disincentives to hospitals to reduce potentially preventable readmissions and complications. MCOs pass incentives and disincentives to hospitals based on a hospital's overall performance for Medicaid clients as calculated by HHSC.	Potentially Preventable Readmissions and Potentially Preventable Complications.	Real time exchange of health information is crucial for care transitions that reduce preventable events. Admission, discharge and transfer data has been demonstrated to reduce preventable hospital admissions and readmissions.
MCO Performance Improvement Projects (PIPs)	Two-year projects designed to follow a common quality improvement cycle. Projects should demonstrate significant improvement sustained over time for clinical and non-clinical care that has a favorable effect on health outcomes and client satisfaction.	HHSC, with the EQRO, determines topics for PIPs based on improvement goals. MCOs create a PIP plan, report on progress annually and provide a final report.	HIE will reduce data lag, promoting the integration of rapid-cycle improvement approaches into the PIPs. Wider use of electronically exchanged clinical data/metrics will expand the range of viable QI projects, particularly collaborative projects.

Initiative	Description	Quality and/or Efficiency Measures	Benefit from Improved Health IT/HIE
Quality Incentive Payment Program (QIPP)	Incentivizes nursing facilities to improve quality and innovation in the provision of services using the CMS five-star rating system as a basis.	Performance measures include: 1) high-risk residents with pressure ulcers; 2) percent of residents who received an antipsychotic medication; 3) residents experiencing one or more falls with major injury; and 4) residents who were physically restrained.	Nursing homes maintain data in electronic format but may not participate in electronic health information exchange with other providers, despite the complex medical backgrounds of their residents. Real time data exchange involving nursing homes is crucial for optimal care coordination and, in particular, will promote better transitions across care settings and higher performance on both nursing home and hospital metrics.
MCO Value-Based Contracting (or Alternative Payment Models) with Providers	HHSC, through contract, requires MCOs to develop value-based payment models with providers.	HHSC has established overall and risk-based targets for the level of MCO reimbursement to providers through value-based payments relative to a plan's total medical expenses.	More clinically relevant data, metrics and data sharing across providers, MCOs and agency programs is needed for the state to fully transition to a value-based Medicaid program.

Appendix C – Public Health Collaborations Advancing Health IT

The Department of State Health Services (DSHS) is Texas' state-level public health agency and is an important component of Texas' Health IT ecosystem. DSHS receives health data from healthcare providers, including general practitioners, specialty care providers and hospitals across the state and uses it to advance DSHS' goals:

- Improve health outcomes through public and population health strategies, including prevention and intervention.
- Optimize public health response to disasters, disease threats and outbreaks.
- Promote the use of science and data to drive decision-making and best practices.

DSHS recognizes the value in using health IT and health information exchange to reduce provider burden in reporting information to the state. It also recognizes the value in transforming the data it receives into timely, accurate, actionable information that supports providers in their delivery of high-quality care to patients.

DSHS is continuously investing in its technology systems that support the state's health IT ecosystem. Key services DSHS provides that rely on the exchange of health information with providers include:

- Operating the State Laboratory, which performs a variety of tests, including newborn blood spot testing.
- Operating the state's immunization registry, which allows healthcare providers and other authorized users to use ImmTrac2 to access immunization histories and vaccination forecasts for children and adults who have consented to have their information included in the immunization registry.
- Disease investigations conducted by the state and local health departments using DSHS' implementation of the National Electronic Disease Surveillance System (NEDSS).
- The Texas syndromic surveillance system, which collects information from hospitals and urgent care centers and makes that information available to local health departments across the state.
- The Texas Cancer Registry, which collects patient-level information from healthcare providers who diagnose and treat cancer. This data can be used to help coordinate patients' care, conduct cancer research and investigate cancer clusters in communities across the state.
- The newborn hearing screening program, which focuses on early detection of hearing issues in newborns and appropriate follow-up care.
- Managing HIV services funded through the Ryan White grant program.

DSHS-run information systems supply actionable information to providers, DSHS program staff, local health departments and other entities. DSHS and its partners use data from these systems to target preventative and early intervention services intended to minimize the health impacts and manage the costs of detected diseases or conditions.

DSHS and HHSC share the same information technology services team, core system architecture requirements, data center and internal IT project approval and governance processes. This sharing eases coordination and helps align resources to meet core needs such as data exchange between the agencies and external partners. This collaboration includes sharing plans and technologies to connect with health information exchanges (HIEs) and other trading partners.

Both DSHS and HHSC will benefit from the improved connectivity for providers and HIEs described in the HIE Implementation Advanced Planning Document. The connection established to support the Emergency Department Encounter Notifications system messages (described in this Plan) between the Texas Health Services Authority's HIETexas and HHSC can also be used to support the exchange of data with DSHS' registries and information systems.

The capabilities provided through the Medicaid provider directory system index being implemented can be extended to serve DSHS' registry systems, reducing duplicative activities by providers and improving DSHS' ability to link information from disparate systems together. Similarly, access to a Medicaid master patient index will be of use to DSHS programs as they match patient records from different systems.

DSHS is working to improve its implementation of NEDSS. Modernizing NEDSS and its affiliated tools will improve providers' ability to submit data, including support for electronic case reporting. The transition to electronic case reporting will reduce manual activities currently required of providers, by enabling direct reporting of conditions from providers' electronic health records (EHRs), leveraging the Reportable Condition Knowledge Management System or similar technologies.

DSHS continues to improve its IT systems, complying with interoperability standards requirements from House Bill 2641, 84th Legislature, Regular Session, 2015, with an aim to provide actionable data to decision-makers at the local, state and national levels. Funding to implement technology changes comes from general revenue, the Centers for Disease Control and Prevention, other grant-making entities and through partnerships with HHSC to implement projects funded through the Advanced Planning Document process.

DSHS recognizes the importance of governance in managing internal systems, the state's health IT ecosystem, as well as at the national level including both exchange networks and messaging standards. Representatives from DSHS are active in all levels of governance and work to ensure that public health's needs, as well as the services it can provide, are recognized.

Attachment No. 6

Acronym List

HEALTHCARE INFORMATION TECHNOLOGY ACRONYMS

- **ACO** – Accountable care organization
- **ADT** – Admission/Discharge/Transfer messages
- **ARRA** – American Recovery and Reinvestment Act
- **BA** – Business associate
- **BAA** – Business Associate Agreement
- **C-CCD** – Continuity of Care Document (CCR + CDA became CCD)
- **C-CDA** – Consolidated Clinical Document Architecture
- **CCR** – Continuity of Care Record; similar in content to a C-CCD
- **CDR** – Clinical Data Repository
- **CE** – Covered entity
- **CHC** – Community Health Center
- **CIO** – Chief Information Officer
- **CISO** – Chief Information Security Officer
- **CMIO** – Chief Medical Information/Informatics Officer
- **CMS** – Centers for Medicare & Medicaid Services; federal agency
- **CPOE** – Computerized physician order entry; orders entered/given electronically
- **CSO** – Chief Security Officer
- **CTO** – Chief Technology Officer
- **DSHS** – Texas Department of State Health Services; public health agency
- **EDEN** – Emergency Department Encounter Notification
- **EH** – Eligible Hospital
- **EP** – Eligible Professional
- **eHEX** – eHealth Exchange; a national HIE network
- **EHR** – Electronic health record
- **ELR** – Electronic Lab Reporting
- **EMR** – Electronic medical record; generally used interchangeably with EHR
- **FACA** – Federal Advisory Committee Act
- **FQHC** – Federally Qualified Health Center; a specific kind of community health center
- **FTP** – File Transport Protocol
- **GHH** – Greater Houston Healthconnect
- **HASA** – Healthcare Access San Antonio
- **HHS** – Department of Health and Human Services; federal agency
- **HHSC** – Texas Health and Human Services Commission
- **HIE** – Health information exchange; generally used interchangeably with HIO
- **HIO** – Health information organization; generally used interchangeably with HIE
- **HIMSS** – Healthcare Information Management Systems Society
- **HIPAA** – Health Insurance Portability and Accountability Act of 1996
- **HISP** – Health information service provider

- **HIT** – Health information technology
- **HITECH** – Health Information Technology for Economic and Clinical Health Act
- **HL7** – Health Level 7; non-profit standards developing organization
- **IAPD** – Implementation Advance Planning Document
- **ICC** – Integrated Care Collaboration
- **ICD-10** – International Classification of Diseases, 10th Revision
- **ISO** – International Standards Organization
- **MACRA** – Medicare Access and CHIP Reauthorization Act of 2015
- **MIPS** – Merit-Based Incentive Payment System
- **MU** – Meaningful Use
- **OCR** – HHS Office for Civil Rights; enforces HIPAA
- **ONC** – Office of the National Coordinator for Health Information Technology
- **P4P** – Pay for performance; quality performance payment model
- **PDMP** – Prescription Drug Monitoring Program
- **PdN** – Paso del Norte HIE; (now known as "PHIX")
- **PHI** – protected health information
- **PHR** – Personal Health Record
- **PIA** – Texas Public Information Act
- **PULSE** – Patient Unified Lookup System for Emergencies
- **REC** – Regional extension center
- **RFA** – Request for Applications
- **RFI** – Request for Information
- **RFP** – Request for Proposals
- **RFQ** – Request for Qualifications
- **RGV HIE** – Rio Grande Valley Health Information Exchange
- **SAMHSA** – Substance Abuse and Mental Health Services Administration
- **SAML** – Security Assertion Markup Language
- **sFTP** – Secure File Transport Protocol
- **SOAP** – Simple Object Access Protocol
- **SDO** – Standards developing organization
- **SOW** – Statement of Work
- **TAHIO** – Texas Association of Health Information Organizations
- **THA** – Texas Hospital Association
- **TMA** – Texas Medical Association
- **VA** – Veterans Administration
- **VHA** – Veterans Health Administration
- **XML** - Extensible Markup Language

Attachment No. 7

List of Disclosed Interests

THSA LIST OF INTERESTS

Name	Interests
Shannon Calhoun	None
Paula Anthony-McMann	• Healthcare Information Management Systems Society – member • Academy of Human Resource Development – member • American College of Healthcare Executives – fellow • Texas Hospital Association Foundation – board member • Syndeti, LLC – President (UT Health East Texas is a current client) • Next Wave Health Advisors – Contract Consultant • The University of Texas at Tyler – Adjunct Faculty
Carlos Vital	• Member of Texas Medical Association • Member of Harris County Medical Society • Member of Greater Houston Allergy & Immunology Society • Member of South Texas Independent Allergy • Member of Houston Medical Forum • Member of National Medical Association • Assistant Clinical Professor at Texas A&M Medical School Houston, TX • Xolair Speaker for Genentech, Compensated • Fellow, AAAAI • Fellow, ACAAI
Emily Hartmann	• Paso del Norte Health Information Exchange – Employee • HIMSS Lubbock Chapter – President of Board of Directors • Strategic HIE Collaborative (SHIEC) – PHIX is a member • eHealth Exchange – PHIX is a Participant • Texas Tech University Health Sciences Center El Paso – Spouse and Mother are employees
Jeff Hoogheem	None
Jerome Lisk	• Texas Medical Association • American Academy of Neurology • University of Texas Health Science Center at Tyler • Christus Trinity Mother Frances Hospital
Kenneth James	• Texas Association of Health Plans – member through Superior
Leticia Rodriguez	None
Siobhan Shahan	None
Jonathan Sandstrum Hill	None
Calvin Green	None listed
Lourdes Cuellar	None listed
Victoria Bryant	None listed

Salil Deshpande	• Member of American Medical Association; American College of Physicians; Harris County Medical Society; Texas Medical Association • Member of Statewide Health Coordinating Council; Texas Health and Human Services Commission's Medical Care Advisory Committee, Drug Utilization Review Board, and e-Health Advisory Committee • Member of the Board of Directors of: Greater Houston Area March of Dimes; The Living Bank; UnitedHealthcare of Texas • Employed by UnitedHealthcare, which has contractual relationships with Texas-based Health Information Exchanges

STAFF MEMBER INTERESTS	
Name	**Interests**
George Gooch	• Health Care Compliance Association – Member • International Association of Privacy Professionals – Member
Eric Heflin (*contractor*)	• Sequoia Project – employee/CTO and CIO • IHE USA – Board member • IHE International – former board member
Annie Nabers	None
Stephen Raines	None

TEXAS HEALTH SERVICES AUTHORITY

STAKEHOLDER INTERESTS – 2019

Pursuant to Section 182.053, Health & Safety Code, the governor shall appoint individuals representing the following stakeholder groups to the THSA board of directors:

- Texas local health information exchanges
- Consumers
- Clinical laboratories
- Health benefit plans
- Hospitals
- Regional health information exchange initiatives
- Pharmacies
- Physicians
- Rural health providers
- Any other area the governor finds necessary

Below are the larger healthcare/technology trade associations in the state that many of the above-referenced board members are affiliated with.

Entity	Policies that relate to "THSA or statewide HIE"?
Texas Hospital Association (THA)	None
Texas Medical Association (TMA)	"19. State support for HIE is important. However, state government's primary role should be to foster coordination of HIE efforts, including providing access to funding or other financial incentives that promote the adoption of health information technologies. 20. TMA physicians should support partnerships with nongovernmental entities developing HIE solutions with minimal mandates, but only where it leads to physicians' stewardship of the data they produce, and patients' control over data that may identify them (CPMS Rep. 3-A-07)."
Texas Association of Health Plans (TAHP)	None
Texas Association of Health Information Organizations (TAHIO)	None

Texas Organization of Rural & Community Hospitals (TORCH)	None
Texas eHealth Alliance (TeHA)	"Priority #4- Adoption, Regulation, Oversight, and Coordination of Healthcare IT. We support legislation that enables the efficiencies of free-market forces constrained only by appropriate privacy and confidentiality considerations to promote quality of care and/or reduce cost of care. This specifically includes support for: -The mission of the Texas Health Services Authority: to promote and coordinate the development of a seamless electronic health information infrastructure to improve the quality, safety, and efficiency of the Texas health care sector while protecting individual privacy. -Legislation that removes statutory barriers to, or promotes and develops, the widespread adoption of HIE, e-prescribe and electronic medical records. This includes information technology systems at HHS agencies that interface with provider systems using nationally recognized standards to facilitate data sharing, as well as appropriate program and data analysis. -Legislation that encourages the HHS agencies to be full participants in state level health information exchange activities and actively seek opportunities to improve their programs and infrastructure through HIE. -Legislation that encourages innovation in health care service delivery, shortens the time to implementation of new technology-supported approaches to program management, and enables the ability of digital tools to support value-based purchasing."