Health Information Exchange ("HIE") Texas ("HIETexas") State-Level Trust Agreement

This Health Information Exchange ("HIE") Texas ("HIETexas") State-Level Trust Agreement (hereinafter the "HIETexas Agreement" or the "Agreement") is entered into as of the Effective Date (defined below), by and between the undersigned participants (hereinafter each referred to individually as "Participant" and collectively as "Participants") and the Texas Health Services Authority ("THSA").

RECITALS

WHEREAS, in 2007, the Texas State Legislature created the THSA pursuant to Chapter 182 of the Texas Health and Safety Code in order to "promote, implement, and facilitate the voluntary and secure exchange of health information," by establishing statewide health information exchange capabilities and "promoting definitions and standards for electronic interactions statewide;" and

WHEREAS, in March 2010, the Office of National Coordinator for Health Information Technology ("ONC") awarded the Texas Health and Human Services Commission ("HHSC") with funding through the American Recovery and Reinvestment Act's ("ARRA") State HIE Cooperative Agreement Program to fund state planning and implementation of electronic health information networks. The HHSC serves as the fiscal agent for this funding, and THSA, under contract with HHSC, has developed HIE strategic and operational plans for Texas that were approved by the ONC in November 2010; and

WHEREAS, HIETexas is a network of connections between health care providers and other participants in Texas that operates for the purpose of facilitating the private and secure sharing of health data in accordance with Applicable law.

WHEREAS, HIETexas plans to participate in national electronic health information exchanges, such as the eHealth Exchange (formerly known as the Nationwide Health Information Network), by executing on behalf of itself and its Participants the eHealth Exchange's Data Use and Reciprocal Support Agreement ("DURSA"), as may be amended from time to time;

WHEREAS, all undersigned Participants facilitate and govern the exchange of Health Data (as defined below) among groups of persons or organizations that wish to request and/or receive Health Data from other Participants in HIETexas;

WHEREAS, as a condition of participation in HIETexas, all Participants must enter into this Agreement for purposes of electronic data exchange; and

WHEREAS, the purpose of this Agreement is to provide a legal framework for enabling Participants to exchange Health Data through HIETexas.

NOW, THEREFORE, for and in consideration of the mutual covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Participants mutually agree as follows:

1. DEFINITIONS

For the purposes of this Agreement, the following terms shall have the meaning ascribed to them below. All defined terms are capitalized throughout this Agreement.

a. **Applicant** shall mean anyone that submits an application to become an HIETexas Participant.

b. **Applicable Law** means all applicable statutes and regulations of the State(s) or jurisdiction(s) in which the Participant operates, as well as all applicable Federal statutes, regulations, standards and policy requirements.

c. **Authorization** shall have the meaning and include the requirements set forth at 45 C.F.R. § 164.508 of the HIPAA Regulations and include any similar but additional requirements under Applicable Law.

d. **Adverse Security Event** shall mean the unauthorized acquisition, access, disclosure, or use of unencrypted Message Content in the process of being transacted in a manner permitted by this Agreement by anyone who is not a Participant or Participant User of by a Participant or Participant User in any manner that is not a Permitted Purpose under this Agreement. For the avoidance of doubt, an "Adverse Security Event" under this Agreement does not include the following:

1. any unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of a Participant or Participant User if:

.01. such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participant or Participant User; and

.02. such unencrypted Message Content is not further acquired, accessed, disclosed or used by such employee or individual; or

2. any acquisition, access, disclosure or use of information contained in or available through the Participant's System where such acquisition, access, disclosure or use was not directly related to Transacting Message Content.

e. **Business Associate** shall have the meaning set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations.

f. **Common Participant Resources** shall mean software, utilities and automated tools made available for use in connection with the Transaction of Message Content pursuant to this Agreement and that have been officially designated as "Common Participant Resources" by the THSA.

g. **Confidential Participant Information**, for the purposes of this Agreement, shall mean proprietary or confidential materials or information of a Discloser in any medium or format that a Discloser labels as such upon disclosure. Confidential Participant Information includes, but is not limited to: (i) the Discloser's designs, drawings, procedures, trade secrets, processes, specifications, source code, System architecture, security measures, research and development, including, but not limited to, research protocols and findings, passwords and identifiers, new products, and marketing plans; (ii) proprietary financial and business information of a Discloser; and (iii) information or reports provided by a Discloser to a Receiving Party pursuant to this Agreement. Notwithstanding any label to the contrary, Confidential Participant Information does not include Message Content; any information which is or becomes known publicly through no fault of a Receiving Party; is learned of by a Receiving Party from a third party entitled to disclose it; is already known to a Receiving Party before receipt from a Discloser as documented by Receiving Party's written records; or, is independently developed by Receiving Party without reference to, reliance on, or use of, Discloser's Confidential Participant Information. Message Content is excluded from the definition of Confidential Participant Information because other provisions of this Agreement address the appropriate protections for Message Content.

h. **Covered Entity** shall have the meaning set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations. For avoidance of doubt, although the term "covered entity" is much more broadly defined by Chapter 181 of the Texas Health and Safety Code pertaining to Medical Records Privacy, this broader definition does not apply to this Agreement except to the extent that any covered entities, as defined by Chapter 181, are required to comply with the applicable provisions of that Chapter.

i. **Digital Credentials** shall mean a mechanism that enables Participants to electronically prove their identity and their right to Transact Message Content with other Participants as further defined in the HIETexas Operating Policies and Procedures.

j. **Discloser** shall mean a Participant that discloses Confidential Participant Information to a Receiving Party.

k. **Dispute** shall mean any controversy, dispute, or disagreement arising out of or relating to this Agreement.

l. **Effective Date** shall mean the date specified in Section 23.12 of this Agreement.

m. **Governmental Participants** shall mean collectively those Participants that are local, state or Federal agencies.

n. **Health Care Operations** shall have the meaning set forth at 45 C.F.R. §164.501 of the HIPAA Regulations.

o. **Health Care Provider** shall have the meaning set forth at 45 C.F.R. §160.103 of the HIPAA Regulations.

p. **Health Information Service Provider or HISP** shall mean a company or other organization that will support one or more Participants by providing them with operational, technical, or health information exchange services.

q. **Health Plan** shall have the meaning set forth at 45 C.F.R. §160.103 of the HIPAA Regulations.

r. **HIETexas** shall mean the data sharing network which was developed by the Texas Health Services Authority under Chapter 182, Texas Health and Safety Code, and consists of governmental and non-governmental exchange partners who share information under a multi-purpose set of standards and services which are designed to support a broad range of information exchange activities using various technical platforms and solutions.

s. **HIPAA Regulations** means the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164) promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as in effect on the Effective Date of this Agreement and as may be amended, modified, or renumbered.

t. **Joinder Agreement** shall mean, with respect to Participants, the agreement that each New Participant signs to be bound by this Agreement. The Joinder Agreements for New Participants is located at Attachment 4 of this Agreement.

u. **Message** shall mean an electronic transmission of Message Content Transacted between Participants using the Specifications. Messages are intended to include all types of electronic transactions as specified in the Performance and Service Specifications, including the data or records transmitted with those transactions.

v. **Message Content** shall mean that information contained within a Message or accompanying a Message using the Specifications. This information includes, but is not limited to, Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. §164.514), individually identifiable information, pseudonymized data, metadata, Digital Credentials, and schema. For avoidance of doubt, information exchanged between participants that is not Transacted using the Specifications, and that does not utilize any state shared services for the purpose of Transacting information, is not subject to this Agreement, and participants are free to contract separately with regard to the use of such information to the extent permitted by Applicable Law.

w. **Network** shall mean HIETexas.

x. **Network Utilities** shall mean any shared infrastructure used to facilitate the transmission of Message content for the Network including, but not limited to, gateway services, healthcare directory, master patient indices, record locator services.

y. **New Participant** shall mean an organization or agency that is approved as a Participant by the THSA pursuant to the Operating Policies and Procedures and Section 23.03 of this Agreement.

z. **Non-Governmental Participants** shall mean collectively those Participants which are not Governmental Participants.

aa. **Notice or Notification** shall mean a written communication, unless otherwise specified in this Agreement, sent to the appropriate Participant's representative at the address listed on the THSA website. It is the Participant's responsibility to ensure that its contact information on the THSA website is up to date and correct.

bb. **ONC** shall mean the Office of the National Coordinator for Health Information Technology in the Office of the Secretary, U.S. Department of Health and Human Services.

cc. **Operating Policies and Procedures** shall mean the policies and procedures adopted by the THSA that describe (i) management, operation and maintenance of the Performance and Service Specifications; (ii) qualifications, requirements and activities of Participants when Transacting Message Content with other Participants; and (iii) support of the Participants who wish to Transact Message Content with other Participants. The Operating Policies and Procedures are attached hereto as Attachment 1, as amended from time to time in accordance with Section 11.03.

dd. **Participant** shall mean any (i) organization that oversees and conducts, on its own behalf and/or on behalf of its Participant Users, electronic transactions or exchanges of health information among groups of persons or organizations; (ii) federal, state, tribal or local governments, agencies or instrumentalities that need to exchange health information with others as part of their official function; (iii) organization that supports program activities or initiatives that are involved in healthcare in any capacity and has the technical ability to meet the applicable Performance and Service Specifications to electronically transact health information on its own behalf or on behalf of its Participant Users; or (4) has the organizational infrastructure and legal authority to comply with the obligations in this Agreement and to require their Participant Users to comply with applicable requirements in this Agreement. Participants may act as a Submitter, Recipient or both when Transacting Message Content.

ee. **Participant Access Policies** means those policies and procedures of a Participant that govern the Participant Users' ability to transact information using the Participant's system including, but not limited to, the Transaction of Message Content.

ff. **Participant User** means any person who has been authorized to Transact Message

Content through the respective Participant's System in a manner defined by the respective Participant. "Participant Users" may include, but are not limited to, Health Care Providers; Health Plans; individuals whose health information is contained within, or available through, a Participant's System; and employees, contractors, or agents of a Participant. A Participant User may act as a Submitter, a Recipient or both when Transacting Message Content.

gg. **Payment** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

hh. **Performance and Service Specifications** shall mean the Specifications, as well as any implementation guidance, migration plans and other technical materials and resources approved by the THSA in accordance with Section 10.03 of this Agreement.

ii. **Permitted Purpose** means one of the following reasons for which Participants or Participant Users may legitimately Transact Message Content, subject to any additional restrictions contained in Applicable Law:

1. Treatment, Payment, Health Care Operations, and Authorization-based disclosures as defined by HIPAA;

2. Transaction of Message Content related to value based payment models, alternative payment arrnagements or financial risk sharing models of any nature whether for Medicare, Medicaid, other federal programs, commercial payers or employer self-insured arrangements. This could include, but is not limited to, participation in Medicare bundled payments, the Medicare Shared Savings Program, other Medicare Alternative Payment programs, Medicaid Managed Care programs or commercial value-based payment programs;

3. Transaction of Message Content for certain specialized government functions which are necessary to fulfill an agency's statutory obligations for programs the agency administers including, but not limited to: (i) activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission; (ii) for the purpose of the Department of Veterans Affairs determining the individual's eligibility or entitlement to benefits under the VA upon separation or discharge of the individual from military service; (iii) to determine eligibility for or entitlement to or provision of other government benefits; (iv) for activities related to eligibility for or enrollment in a health plan that is a government program; (v) for administering a government program providing public benefits, to coordinate covered functions; or (vi) to improve administration and management relating to the covered functions of such government programs;

4. Public health activities and reporting as permitted by Applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514(e);

5. Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered

Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content under this Agreement, provided that the purpose is not otherwise described in subsections 1-4 of this definition and the purpose is permitted by Applicable Law, including but not limited to the HIPAA regulations. "Meaningful use of certified electronic health record technology" shall have the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102; and

6. Transaction of Message Content in support of an individual's: (i) right to access their health information or (ii) right to direct with whom their information can be shared or where their information should be sent. For the avoidance of doubt, a Participant may be prevented from disclosing information due to Applicable Law even though the individual asserts this Permitted Purpose.

The THSA and all Participants acknowledge that some Participants may have policies, procedures or agreements in place that are more restrictive than the Permitted Purposes in this Agreement and in such cases, Participants will not Transact Message Content for all Permitted Purposes.

jj. **Protected Health Information or PHI** shall have the meaning set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations.

kk. **Receiving Party** shall mean a Participant that receives Confidential Participant Information in any capacity from a Discloser.

ll. **Recipient** shall mean the Participant(s) or Participant User(s) that receives Message Content through a Message from a Submitter for a Permitted Purpose. For purposes of illustration only, Recipients include, but are not limited to, Participants or Participant Users who receive queries, responses, subscriptions, publications or unsolicited Messages.

mm. **Specifications** means the specifications adopted by the THSA pursuant to this Agreement to prescribe the data content, technical, and security requirements to enable the Participants to Transact Message Content. Specifications may include, but are not limited to, specific HIETexas standards, services and policies. The Specifications are published on THSA.org, and may be amended from time to time in accordance with Sections 10.02 and 10.03.

nn. **Submitter** shall mean the Participant(s) or Participant User(s) who submits Message Content through a Message to a Recipient for a Permitted Purpose. For purposes of illustration only, Submitters include, but are not limited to, Participants or Participant Users who push Messages with Message Content, send Messages seeking Message Content, send Messages in response to a request, send subscription Messages, or publish Messages with Message Content in response to subscription Messages.

oo. **System** shall mean software, portal, platform, or other electronic medium controlled by a Participant through which the Participant conducts its health information exchange related activities. For purposes of this definition, it shall not matter whether the Participant controls the software, portal, platform, or medium through ownership, lease, license, or otherwise.

pp. **Testing** shall mean to send, request, receive, assert, respond to, submit, route, subscribe to, or publich Message Content using the Performance and Service Specifications.

qq. **Transact** means to send, request, receive, assert, respond to, submit, route, subscribe to, or publish Message Content using the Performance and Service Specifications.

rr. **Transaction Pattern** shall mean a type of information exchange service(s) enabled by the Specifications. The Validation Plan will identify the Transaction Pattern(s) and the Specifications required to implement each Transaction Pattern. The Transaction Patterns may be amended from time to time through amendment of the Specifications and the Operating Policies and Procedures.

ss. **Treatment** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

tt. **Use Case** shall mean a particular activity involving Transacting Message Content using the Network in order to support a specific function or facilitate an identified outcome.

uu. **Validation Plan** shall mean the framework for Testing and demonstrations for parties seeking to become Participants. The Validation Plan is attached hereto as Attachment 6, and as amended from time to time in accordance with Section 10.02 and 10.03.

2. **Reserved.**

3. **Reserved.**

4. **Administration of HIETexas**.

4.0 **THSA Obligations.** The Participants hereby grant the THSA the right and the THSA agrees to provide oversight, facilitation and support for the Network by conducting activities including, but not limited to, the following:

a. Determining whether to admit a New Participant in accordance with the Operating Policies and Procedures;

b. Maintaining a definitive list of all Transaction Patterns and volumes per Transaction Pattern supported by each of the Participants;

c. Evaluating requests for and approving new Use Cases;

d. Developing and amending Operating Policies and Procedures in accordance with Section 11 of this Agreement;

e. Receiving reports of Adverse Security Events and acting upon such reports in accordance with Section 14.03 of this Agreement (Adverse Security Event Notification);

f. Suspending or terminating Participants in accordance with Section 19 of this Agreement (Suspension and Termination);

g. Resolving Disputes between Participants in accordance with Section 21 of this Agreement (Dispute Resolution);

h. Managing the amendment of this Agreement in accordance with Section 23.02 of this Agreement;

i. Approving the adoption of Network Utilities;

j. Evaluating, prioritizing and adopting new Performance and Service changes to Specifications, existing Performance and Service Specifications in accordance with Section 10 of this Agreement;

k. Maintaining a process for managing versions of the Performance and Service Specifications, including migration planning;

l. Coordinating with ONC to help ensure the interoperability of the Performance and Service Specifications with other health information exchange initiatives including, but not limited to, providing input into the broader ONC specifications activities and ONC Standards and Interoperability Framework initiatives;

m. Entering into agreements to broaden access to data to enhance connectivity across platforms and networks as provided in accordance with Operating Policies and Procedures which shall include an express opt-out right for every Participant;

n. Conducting studies from time to time related to various issues surrounding HIETexas including, but not limited to, any project evaluation required under grants or contracts and/or the efficacy and usefulness of HIETexas; and

o. Fulfilling all other responsibilities delegated by the Participants to the THSA as set forth in this Agreement.

5. **Use of Message Content**.

5.01. **Permitted Purpose**. Participants may Transact Message Content only for a Permitted Purpose as defined in this Agreement. Each Participant shall require that its Participant Users comply with this Section 5.01.

5.02. **Permitted Future Uses.** Subject to this Section 5.02 and Section 19.07, Recipients may retain, use and re-disclose Message Content in accordance with Applicable Law and the Recipient's record retention policies and procedures. If the Recipient is a

Participant that is a Business Associate of its Participant Users, such Participant may retain, use and re-disclose Message Content in accordance with Applicable Law and the agreements between the Participant and its Participant Users.

5.03. **Management Uses**. The THSA may request information from Participants, and Participants shall provide requested information, for the purposes listed in Section 4.0 of this Agreement.

6. **System Access Policies**.

6.01. **Autonomy Principle**. Each Participant shall have Participant Access Policies. Each Participant acknowledges that Participant Access Policies will differ among them as a result of differing Applicable Law and business practices. Each Participant shall be responsible for determining whether and how to Transact Message Content based on the application of its Participant Access Policies to the information contained in the Message. The Participants agree that each Participant shall comply with the Applicable Law, this Agreement, its own policies, procedures and agreements, and all applicable Performance and Service Specifications in Transacting Message Content.

6.02. **Identification**. Each Participant shall employ a process by which the Participant, or its designee, validates sufficient information to uniquely identify each person seeking to become a Participant User prior to issuing credentials that would grant the person access to the Participant's System.

6.03. **Authentication**. Each Participant shall employ a process by which the Participant, or its designee, uses the credentials issued pursuant to Section 6.02 to verify the identity of each Participant User prior to enabling such Participant User to Transact Message Content.

7. **Enterprise Security**.

7.01. **General**. Each Participant and THSA shall be responsible for maintaining a secure environment within systems that store PHI and/or are used in transacting Message Content through HIETexas that supports the operation and continued development of the Performance and Service Specifications. Participants shall use appropriate safeguards to prevent use or disclosure of Message Content other than as permitted by this Agreement, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Message Content. Appropriate safeguards for Participants and THSA shall be those identified in the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, as safeguards, standards, "required" implementation specifications, and "addressable" implementation specifications to the extent that the "addressable" implementation specifications are reasonable and appropriate in the Participant's and THSA's environment. If an "addressable" implementation specification is not reasonable and appropriate in the Participant's or THSA's environment, then the Participant or THSA must document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if

reasonable and appropriate. Appropriate safeguards for Federal Participants shall be those required by Applicable Law related to information security. Each Participant and THSA shall, as appropriate under either the HIPAA Regulations, or under Applicable Law, have written privacy and security policies in place by the Participant's respective Effective Date. Participants and THSA shall also be required to comply with any Performance and Service Specifications or Operating Policies and Procedures adopted by the THSA, respectively, that define requirements and expectations for Participants and THSA with respect to enterprise security, which may or not be in excess of those requirements under the HIPAA Security Rule.

7.02. **Malicious Software**. Each Participant shall ensure that it employs security controls that meet applicable industry or Federal standards so that the information and Message Content being Transacted and any method of Transacting such information and Message Content will not introduce any viruses, worms, unauthorized cookies, trojans, malicious software, malware, or other program, routine, subroutine, or data designed to disrupt the proper operation of a System or any part thereof or any hardware or software used by a Participant in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause a System or any part thereof or any hardware, software or data used by a Participant in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable. In the absence of applicable industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this Section.

8. **Equipment and Software**. Each Participant shall be responsible for procuring all equipment and software that are necessary for it and its authorized agents, employees and independent contractors to Transact Message Content. Each Participant shall ensure that all computers and electronic devices owned or leased by the Participant and its agents, employees, and independent contractors to be used to Transact Message Content are properly configured, including, but not limited to, the base workstation operating system, web browser, and Internet connectivity.

9. **Monitoring and Auditing**. The THSA, acting through its agents and independent contractors, in order to confirm compliance with this Agreement, shall have the right, but not the obligation, to monitor and audit Network exchange activities. Unless prohibited by Applicable Law or, in the case of a Governmental Participant that Participant's policies or internal guidelines that it has adopted in the normal course of business, Participant agrees to cooperate with the THSA in these monitoring and auditing activities and to provide, upon the reasonable request of the THSA, information in the furtherance of the THSA's monitoring and auditing including, but not limited to, audit logs of exchange transactions and summary reports of exchange activities, to the extent that Applicant possesses such information. Each Participant represents that, through its agents, employees, and independent contractors, it shall have the ability to monitor and audit all access to and use of its System related to this Agreement, for system administration, security, and other legitimate purposes. Each Participant shall perform those auditing activities required by the Performance and Service Specifications.

10. **Performance and Service Specifications**.

10.01. **General Compliance.**

a. **Transaction Patterns.** Each Participant shall implement and maintain at least one Transaction Pattern as a Submitter, a Recipient or both. Each Participant shall implement and maintain a Transaction Pattern only after appropriate approval and validation by the THSA in accordance with the Operating Policies and Procedures.

b. **Performance and Service Specifications**. Each Participant shall comply with (i) all of the Performance and Service Specifications applicable to the Transaction Pattern(s) that the Participant implements and maintains; and (ii) those Performance and Service Specifications identified by the THSA as applicable to all Participants.

10.02. **Adoption of Performance and Service Specifications**. The Participants hereby grant the THSA or its designee the right to adopt new Performance and Service Specifications, and to adopt amendments to, or repeal and replacement of, the Performance and Service Specifications at any time through the Performance and Service Specification Change Process described in Section 10.03.

10.03. **Performance and Service Specification Change Process**.

a. **Collaborative Review Process**. Unless required due to changes in Applicable Law or necessitated to maintain the stability of the HIETexas due to an emergency circumstance(s), prior to approving any new, amended, repealed or replaced Performance and Service Specification, the THSA shall solicit and consider comments from the applicable THSA Task Forces and the THSA Collaboration Council, in consultation with the THSA Board and HHSC as appropriate. If a change is made without soliciting and considering comments and is not required by a change in Applicable Law, the THSA will engage Participants in a collaborative process regarding the change as soon as practicable.

b. **Participant Duty to Terminate Participation**. If, as a result of a change made by the THSA in accordance with this Section 10.03, a Participant will not be able to comply with the relevant Performance and Service Specifications or does not otherwise desire to continue to Transact Message Content with other Participants after such change becomes effective, then such Participant shall terminate this Agreement accordance with Section 19.02. This does not preclude a Participant from continuing participation in HIETexas if the Participant cannot or will not comply with changes to the specifications regarding Transaction Patterns that the Participant has agreed not to enable through its Participation Agreement with THSA.

11. **Operating Policies and Procedures**.

11.01. **General Compliance.** Each Participant shall comply with the Operating Policies and Procedures adopted by the THSA in accordance with this Agreement for messages

transacted between HIETexas and Participant.

11.02. **Development of the Operating Policies and Procedures.** THSA shall develop new Operating Policies and Procedures, and amend, or repeal and replace, the Operating Policies and Procedures at any time through the Operating Policies and Procedures Change Process described in Section 11.03.

11.03. **Operating Policies and Procedures Change Process**. Unless required due to changes in Applicable Law or necessitated to maintain the stability of the HIETexas due to an emergency circumstance(s), prior to approving any new, amended, repealed or replaced Operating Policies and Procedures Change Process, the THSA shall solicit and consider comments from the applicable THSA Task Forces and the THSA Collaboration Council, in consultation with the THSA Board and HHSC.

12. **Expectations of Participants.**

12.01. **Minimum Requirement for Participants that request Message Content for Treatment**. HIETexas exists to promote the seamless exchange of health information across a variety of technical platforms and Health Information Networks. A core principle of eHealth Exchange is that Participants make commitments to the minimum level of data sharing that they will support so that all other Participants can know, and rely on, each Participant's commitment. All Participants that choose to participate in a specific Use Case must comply with all of the Performance and Service Specifications for a Use Case and must take measures to require that its Participant Users comply with all of the Performance and Service Specifications for a Use Case and must take measures to require that its Participant Users comply with all of the Performance and Service Specifications for a Use Case.

a. Participants that request, or allow their respective Participant Users to request, Message Content for Treatment shall have a corresponding reciprocal duty to respond to Messages that request Message Content for Treatment. A Participant shall fulfill its duty to respond by either (i) responding to the Message with the requested Message Content or, (ii) responding with a standardized response that indicates the Message Content is not available or cannot be exchanged. Nothing in this Section 12.01(a) shall require a disclosure that is contrary to a restriction placed on the Message Content by a patient pursuant to Applicable Law.

b. Each Participant that requests, or allows its respective Participant Users to request, Message Content for Treatment shall Transact Message Content with all other Participants for Treatment, in accordance with Sections 6, 12.01(a) and 14 of this Agreement. If a Participant desires to stop Transacting Message Content with another Participant based on the other Participant's acts or omissions in connection with this Agreement, the Participant may temporarily stop Transacting Message Content with such Participant either through modification of its Participant Access Policies or through some other mechanism, to the extent necessary to address the Participant's concerns. If any such cessation occurs, the Participant shall provide a Notification to the THSA

of such cessation and the reasons supporting the cessation, and the THSA shall provide notice to the other Participants regarding such cessation. The Participants shall submit the Dispute leading to the cessation to the Dispute Resolution Process in Section 21. If the cessation is a result of an Adverse Security Event that was reported to, and deemed resolved by, the THSA pursuant to Section 14.03, the Participants involved in the Adverse Security Event and the cessation shall engage in the Dispute Resolution Process in Section 21 in an effort to attempt to reestablish trust and resolve any security concerns arising from the Adverse Security Event.

12.02. **Participant Users and Technology Partners**. For messages transacted to the HIETexas each Participant shall require that all of its Participant Users and Technology Partners Transact Message Content only in accordance with the terms and conditions of this Agreement, including without limitation those governing the use, confidentiality, privacy, and security of Message Content. Each Participant shall discipline appropriately any of its employee Participant Users, or take appropriate contractual action with respect to contractor Participant Users or Technology Partners, who fail to act in accordance with the terms and conditions of this Agreement relating to the privacy and security of Message Content, in accordance with Participant's employee disciplinary policies and procedures and its contractor and vendor policies and contracts, respectively.

12.03. **License to Common Participant Resources.** Participant is hereby granted a nonexclusive, nontransferable, revocable and limited license to any Common Participant Resources solely for use as a Participant in performance of this Agreement. Participant shall not (a) sell, sublicense, transfer, exploit or, other than pursuant to this Agreement, use any Common Participant Resources for Participant's own financial benefit or any commercial purpose, or (b) reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code to any Common Participant Resources. THE COMMON PARTICIPANT RESOURCES ARE PROVIDED —"AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

12.04 **Network Utilities**. The THSA may approve the use of various Network Utilities to support the operation of the Network. If necessary, the THSA may develop an Operating Policy and Procedure for implementation and use of the Network Utility by Participants. The Network Performance and Service Specifications may be updated as needed to effectively implement a Network Utility. The procedures outlined in section 10.03 and 11.03 of this Agreement shall be followed in developing or updating Operating Policies and Procedures or Performance and Service Specifications.

12.05 **Opt-out for new networks**. If the THSA exercises its authority, provided by this Agreement, to enter into agreements to broaden access to data to enhance connectivity across platforms and networks, the Participant may choose to opt-out of

participation in those platforms or networks for any reason. Participant shall provide the THSA written notification of its decision to opt-out. At any time, a Participant may reverse its decision to opt-out.

13. **Specific Duties of a Participant When Submitting a Message**. Whenever a Participant or Participant User acts as a Submitter by submitting a Message to the HIETexas, the Submitter shall be responsible for:

13.01. Submitting each Message in compliance with Applicable Law, this Agreement, the applicable Performance and Service Specifications, its own policies, procedures and agreements, and Operating Policies and Procedures including, but not limited to, representing that the Message is:

(i) for a Permitted Purpose;

(ii) submitted by a Submitter who has the requisite authority to make such a submission;

(iii) supported by appropriate legal authority for Transacting the Message Content including, but not limited to, any consent or Authorization, if required by Applicable Law and Submitter's policies, procedures and agreements; and

(iv) directed to the intended Recipient.

13.02. Representing that assertions or statements related to the submitted Message are true and accurate, if such assertions or statements are required by the Performance and Service Specifications or Operating Policies and Procedures;

13.03. Provide evidence that the Submitter has obtained an Authorization or other evidence of an individual directed transaction, if the Submitter is requesting Message Content from another Participant or Participant User based on the Permitted Purpose described in Section 1ii. Nothing in this Section shall be interpreted as requiring a Submitter who is requesting Message Content to obtain or transmit an Authorization for a request based on a Permitted Purpose other than the one described in Section1ii, even though certain other Participants or Participant Users require such Authorization to comply with Applicable Law.

13.04. For Federal agency Participants only, in addition to complying with Sections 13.01 through 13.03, ensuring that Messages submitted by such Federal Participant adhere to interoperability standards adopted by the Secretary of Health and Human Services, and the National Institute of Standards and Technology ("NIST") and the Federal Information Processing Standards ("FIPS"), as applicable.

13.05 For avoidance of doubt, if a Participant is Transacting Message Content on behalf of a Participant User, Participant shall require Participant User to agree that it will comply with the provisions of sections 13.01 (i-iii) and 13.03 with respect to its submission of the Message to Participant and, if Participant has obtained such assurance from Participant User as required pursuant to this section, Participant is entitled to rely on

Participant User's legally binding representation for purposes of complying with such requirements, unless the Participant has reason to believe that the Participant User is in breach of its agreement with Participant with respect to such representations.

13.06 Participants agree and acknowledge that a response to a request may include, when applicable, a statement that providing such Message Content would be inconsistent with Participant's own policies, procedures, and agreements.

14. **Privacy and Security**.

14.01. **Applicability of HIPAA Regulations**. Message Content may contain PHI. Furthermore, some, but not all, Participants are either a Covered Entity or a Business Associate. To support the privacy, confidentiality, and security of the Message Content, each Participant agrees as follows:

a. If the Participant is a Covered Entity, the Participant does, and at all times shall, comply with the HIPAA Regulations to the extent applicable.

b. If the Participant is a Business Associate of a Covered Entity, the Participant does, and shall at all times, comply with the provisions of its Business Associate Agreements (or for governmental entities relying upon 45 C.F.R. §164.504(e)(3)(i)(A), its Memoranda of Understanding) and Applicable Law.

c. If the Participant is a Governmental Participant, the Participant does, and at all times shall, comply with the applicable privacy and security laws and regulations.

d. If the Participant is neither a Covered Entity, a Business Associate or a Governmental Participant, the Participant shall, as a contractual standard, at all times, at a minimum, comply with the provisions of the HIPAA Regulations set forth in Attachment 2 as if it were acting in the capacity of a Covered Entity or such other standards as decided by the THSA.

14.02. **Business Associate Agreement**. Some Use cases will involve the Transaction of Message Content among Participants, or their Participant Users, that result in a Participant, or Participant User, being considered a Business Associate under the HIPAA Regulations. While this will not be the general rule, when it does occur, the Participants agree that they will enter into a Business Associate Agreement in substantially the same form included in Attachment 5. Compliance with this section's requirements may be satisfied by an existing business associate agreement that includes, at a minimum, the terms listed in Attachment5, by adopting a Business Associate Addendum, in substantially the same form included in Attachment 5, to an existing agreement or by adopting a new Business Associate Agreement in substantially the same form included in Attachment 5.

14.03. **Safeguards**. In accordance with Sections 7, 8 and 9, Participant agrees to use reasonable and appropriate administrative, physical, and technical safeguards and any Performance and Service Specifications and Operating Policies and Procedures to protect

Message Content and to prevent use or disclosure of Message Content other than as permitted by Section 5 of this Agreement.

14.04. **Adverse Security Event Notification**.

a. As soon as reasonably practicable, but no later than five (5) business days after determining that an Adverse Security Event (or "Event") has occurred and is likely to have an adverse impact on the Network or another Participant, Participant shall provide a notification to the THSA and all Participants that are likely impacted by the Event. Participant shall supplement the information contained in the notification as it becomes available and cooperate with other Participants. Notwithstanding the foregoing, Participant agrees that (a) within one (1) hour of learning that an Adverse Security Event occurred and that such Event may involve a Federal Participant, it shall alert the Federal Participant in accordance with the procedures and contacts provided by such Federal Participant, and (b) that within twenty-four (24) hours after determining that an Adverse Security Event has occurred and is likely to have an adverse impact on a Federal Participant(s), Participant shall provide a notification to all such Participants that are likely impacted by the Event, and the THSA, in accordance with the procedures and contacts provided by such Federal Participant. The Notification should include sufficient information for the THSA to understand the nature of the Adverse Security Event. For instance, such Notification could include, to the extent available at the time of the Notification, the following information:

- One or two sentence description of the Adverse Security Event
- Description of the roles of the people involved in the Adverse Security Event (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)
- The type of Message Content involved in the Adverse Security Event
- Participants likely impacted by the Adverse Security Event
- Number of individuals or records impacted/estimated to be impacted by the Adverse Security Event
- Actions taken by the Participant to mitigate any unauthorized access to, use or disclosure of PHI as a result of the Adverse Security Event
- Current Status of the Adverse Security Event (under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar Adverse Security Event.

The Participant shall supplement the information contained in the Notification as it becomes available and cooperate with other Participants and the THSA in accordance with Section 20(e) of this Agreement. The Notification required by this Section 14.04 shall not include any PHI. If, on the basis of the Notification, a Participant desires to stop Transacting Message Content with the Participant that reported an Adverse Security Event, it shall stop Transacting Message Content in accordance with Section 12.01(b) of this Agreement. If, on the

basis of the notification, the THSA determines that (i) the other Participants that have not been notified of the Adverse Security Event would benefit from a summary of the Notification or (ii) a summary of the Notification to the other Participants would enhance the security of the Performance and Service Specifications, it may provide, in a timely manner, a summary to such Participants that does not identify any of the Participants or individuals involved in the Adverse Security Event.

b. Information provided by a Participant in accordance with this Section 14.04, except Message Content, may be Confidential Participant Information. Such Confidential Participant Information shall be treated in accordance with Section16.

c. This Section 14.04 shall not be deemed to supersede a Participant's obligations (if any) under relevant security incident, Adverse Security Event notification or confidentiality provisions of Applicable Law.

d. Compliance with this Section 14.04 shall not relieve Participants of any other security incident or Adverse Security Event reporting requirements under Applicable Law including, but not limited to, HIPAA or those related to consumers.

15. **Representations and Warranties**. Each Participant hereby represents and warrants the following:

15.01. **Accurate Participant Information**. Except to the extent prohibited by Applicable Law, each Participant has provided, and shall continue to provide, the THSA with all information reasonably requested by the THSA and needed by the THSA to discharge its duties under this Agreement or Applicable Law, including during the Dispute Resolution Process. Any information provided by a Participant to the THSA shall be responsive and accurate. Each Participant shall provide Notice to the THSA if any information provided by the Participant to the THSA materially changes. Each Participant acknowledges that the THSA reserves the right to confirm or otherwise verify or check, in its sole discretion, the completeness and accuracy of any information provided by a Participant at any time and each Participant shall reasonably cooperate with the THSA in such actions, given reasonable prior notice.

15.02. **Execution of this Agreement**. Prior to Transacting Message Content with the HIETexas, each Participant shall have executed this Agreement and returned an executed copy of this Agreement to the THSA. In doing so, the Participant affirms that it has full power and authority to enter into and perform this Agreement and has taken whatever measures necessary to obtain all required approvals or consents in order for it to execute this Agreement. The representatives signing this Agreement on behalf of the Participants affirm that they have been properly authorized and empowered to enter into this Agreement on behalf of the Participant.

15.03. **Compliance with this Agreement**. Except to the extent prohibited by Applicable

Law, each Participant shall comply fully with all provisions of this Agreement. To the extent that a Participant delegates its duties under this Agreement to a third party (by contract or otherwise) and such third party will have access to Message Content, that delegation shall be in writing and require the third party, prior to Transacting Message Content with any Participants, to agree to the same restrictions and conditions that apply through this Agreement to a Participant.

15.04. **Agreements with Participant Users.** Each Participant has valid and enforceable agreements with each of its Participant Users that require the Participant User to, at a minimum: (i) comply with all Applicable Law; (ii) reasonably cooperate with the Participant on issues related to this Agreement; (iii) Transact Message Content only for a Permitted Purpose; (iv) use Message Content received from another Participant or Participant User in accordance with the terms and conditions of this Agreement; (v) as soon as reasonably practicable after determining that an Adverse Security Event to the Participant; and (vi) refrain from disclosing to any other person any passwords or other security measures issued to the Participant User by the Participant. Notwithstanding the foregoing, for Participant Users who are employed by a Participant or who are independent contractors of a Participant, compliance with this Section 15.04 may be satisfied through written policies and procedures that address items (i) through (vi) of this Section 15.04 so long as the Participant can document that there is a written requirement that the Participant User must comply with the policies and procedures.

15.05. **Agreements with Technology Partners**. To the extent that a Participant uses technology partners in connection with the Participant's Transaction of Message Content, each Participant affirms that it has valid and enforceable agreements with each of its technology partners, including HISPs, that require the technology partner to, at a minimum: (i) comply with Applicable Law; (ii) protect the privacy and security of any Message Content to which it has access; (iii) as soon as reasonably practicable after determining that an Adverse Security Event occurred, report such Adverse Security Event to the Participant; and (iv) provide services as needed and under the Participant's direction to enable Participant to fulfill responsibilities under this Agreement.

15.06. **Compliance with Specifications, Policies and Procedures.** Each Participant affirms that it fully complies with the Performance and Service Specifications and the Operating Policies and Procedures as more fully discussed in Sections 10.01 and 11.01 of this Agreement.

15.07. **Creation of Test Data**. Participants agree that when testing exchange capabilities with other Participants, Participants shall use only fictitious data to create any test data to be used for testing. Using de-identified PHI for this purpose is not allowed.

15.08. **Accuracy of Message Content**. When acting as a Submitter, each Participant, in accordance with Section 17.02, hereby represents that at the time of transmission, the Message Content it provides is (a) an accurate representation of the data contained in, or available through, its System, (b) sent from a System that employs security controls that meet industry standards so that the information and Message Content being

transmitted are intended to be free from malicious software in accordance with Section 7.02, and (c) provided in a timely manner and in accordance with the Performance and Service Specifications and Operating Policies and Procedures. Other than those representations in Sections 15.07, 15.08 and 15.09, the Submitter makes no other representation, express or implied, about the Message Content.

15.09. **Express Warranty of Authority to Transact Message Content**. To the extent each Participant is a Submitter and is providing Message Content to a Recipient, each Participant represents and warrants that it has sufficient authority to Transact such Message Content.

15.10. **Use of Message Content**. Each Participant hereby represents and warrants that it shall use the Message Content only in accordance with the provisions of this Agreement. Notwithstanding the foregoing, to the extent that the state shared services are required to transmit the data, the data is considered to be Message Content transmitted via this agreement. However, to the extent that the state shared services are not implicated, the Participants are free to enter into separate agreements regarding the transmission of data without reference to this Agreement.

15.11. **Compliance with Laws**. Each Participant shall, at all times, fully comply with all Applicable Law relating to this Agreement, the Transaction of Message Content for a Permitted Purpose and the use of Message Content.

15.12. **Absence of Final Orders.** Each Participant hereby represents and warrants that, as of the Effective Date, it is not subject to a final order issued by any Federal, State, local or international court of competent jurisdiction or regulatory or law enforcement organization, which will materially impact the Participant's ability to fulfill its obligations under this Agreement. Each Participant shall inform the THSA if at any point during the term of this Agreement it becomes subject to such an order.

15.13. **Federal Program Participation.** Each non-Federal Participant hereby represents and warrants that it is not excluded, debarred, or otherwise ineligible from participating in Federal contracts, subcontracts, grants, and non-procurement transactions ("Federal Programs"). Each non-Federal Participant shall immediately provide written Notice to the THSA if it is suspended, proposed for debarment or other exclusion, or otherwise disqualified or declared ineligible from participating in a Federal Program for any reason, or is a party to a legal proceeding that may result in any such action.

16. **Confidential Participant Information**.

16.01. Each Receiving Party shall hold all Confidential Participant Information in confidence and agrees that it shall not, during the term or after the termination of this Agreement, re-disclose to any person or entity, nor use for its own business or benefit, any information obtained by it in connection with this Agreement, unless such use or re-disclosure is permitted by the terms of this Agreement.

16.02. Confidential Participant Information may be re-disclosed as required by operation of law, such as pursuant to an order of a court or governmental body, provided that the Receiving Party immediately notifies the Discloser of the existence, terms and

circumstances surrounding such operation of law to allow the Discloser its rights to object to such disclosure. If after Discloser's objection, the Receiving Party is still required by operation of law to re-disclose Discloser's Confidential Participant Information, it shall do so only to the minimum extent necessary to comply with the operation of the law and shall request that the Confidential Participant Information be treated as such.

17. **Disclaimers**.

17.01. **Reliance on a System**. Each Participant acknowledges and agrees that: (i) the Message Content provided by, or through, its System is drawn from numerous sources, and (ii) it can only confirm that, at the time Message Content is Transacted, the information and Message Content Transacted are an accurate representation of data contained in, or available through, its System. Nothing in this Agreement shall be deemed to impose responsibility or liability on a Participant related to the clinical accuracy, content or completeness of any Message Content provided pursuant to this Agreement. The Participants acknowledge that other Participants' Digital Credentials may be activated, suspended or be required to be revoked at any time or the Participant may suspend its participation; therefore, Participants may not rely upon the availability of a particular Participant's Message Content.

17.02. **Incomplete Medical Record**. Each Participant acknowledges that Message Content Transacted by Participants may not include the individual's full and complete medical record or history. Such Message Content will only include that data which is the subject of the Message and available for exchange among Participants.

17.03. **Patient Care.** Message Content obtained through a Message is not a substitute for any Participant or Participant User, if that person/entity is a Health Care Provider, obtaining whatever information he/she/it deems necessary, in his/her professional judgment, for the proper treatment of a patient. The Participant or Participant User, if he/she/it is a Health Care Provider, shall be responsible for all decisions and actions taken or not taken involving patient care, utilization management, and quality management for his/her/its respective patients and clients resulting from, or in any way related to, the use of the HIETexas standards, services and policies agreed to by the Participants pursuant to this Agreement or the Message Content made available thereby. None of the Participants, by virtue of executing this Agreement, assume any role in the care of any patient other than meeting their responsibilities in the secure exchange of Messages.

17.04. **Carrier lines**. All Participants acknowledge that the Transaction of Message Content between Participants is to be provided over various facilities and communications lines, and information shall be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, carrier lines) owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which may be beyond the Participants' control. Provided a Participant uses reasonable security measures, no less stringent than those directives, instructions, and specifications contained in this Agreement, the Performance and

Service Specifications, and the Operating Policies and Procedures, the Participants assume no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted over those carrier lines, which are beyond the Participants‘ control, or any delay, failure, interruption, interception, loss, transmission, or corruption of any Message Content or other information attributable to transmission over those carrier lines which are beyond the Participants‘ control. Use of the carrier lines is solely at the Participants’ risk and is subject to all Applicable Law.

17.05 **Third Party Technology**. All Participants acknowledge that other Participants use technology solutions, applications, interfaces, software, platforms, clearinghouses and other IT resources to support exchange of message content that may be provided by third parties (Third Party Technology). Each Participant shall have agreements in place that require Third Party Technology vendors to provide reliable, stable and secure services to the Participant. However, all Participants acknowledge that Third Party Technology may be non-functional or not available at times and that this could prevent a Participant from Transacting Message Content. Participants do not make any representations or warranties as to their Third Party Technology.

17.06. **No Warranties**.

EXCEPT AS REPRESENTED IN SECTIONS 13.02 AND 15.08, MESSAGE CONTENT IS PROVIDED “AS IS” AND “AS AVAILABLE” WITHOUT ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IT IS EXPRESSLY AGREED THAT IN NO EVENT SHALL THE PARTICIPANT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUES, LOSS OF USE, OR LOSS OF INFORMATION OR DATA, WHETHER A CLAIM FOR ANY SUCH LIABILITY OR DAMAGES IS PREMISED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER THEORIES OF LIABILITY, EVEN IF THE PARTICIPANT HAS BEEN APPRISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES OCCURRING. THE PARTICIPANT DISCLAIMS ANY AND ALL LIABILITY FOR ERRONEOUS TRANSMISSIONS AND LOSS OF SERVICE RESULTING FROM COMMUNICATION FAILURES BY TELECOMMUNICATION SERVICE PROVIDERS OR OTHER THIRD PARTIES.

THE SPECIFICATIONS, INCLUDING ANY PERFORMANCE AND SERVICE SPECIFICATIONS, AS WELL AS THE OPERATING POLICIES AND PROCEDURES PROVIDED AS ATTACHMENTS TO THIS AGREEMENT, AS MAY BE AMENDED FROM TIME TO TIME PURSUANT TO THE PROVISIONS OF THIS AGREEMENT (THE “DOCUMENTS”) ARE INTENDED AS A GUIDE TO HELP FACILITATE HEALTH INFORMATION EXCHANGE RATHER THAN AN EXHAUSTIVE LIST OF TECHNOLOGICAL COMPONENTS

REQUIRED TO PARTICIPATE IN AN EXCHANGE. AS SUCH, THESE DOCUMENTS ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IT IS EXPRESSLY AGREED THAT IN NO EVENT SHALL THE THSA, ITS OFFICERS, DIRECTORS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUES, LOSS OF USE, OR LOSS OF INFORMATION OR DATA, WHETHER A CLAIM FOR ANY SUCH LIABILITY OR DAMAGES IS PREMISED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER THEORIES OF LIABILITY, EVEN IF THE THSA HAS BEEN APPRISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES OCCURRING. THE THSA DISCLAIMS ANY AND ALL LIABILITY FOR ERRONEOUS, INCOMPLETE OR FAILRED TRANSMISSIONS RELATED TO THE DOCUMENTS OR ANY PARTICANT'S IMPLEMENTATION OF SUCH DOCUMENTS.

17.07. **Performance of the HIETexas Standards, Services and Policies.** The Participant makes no representation, express or implied, as to the performance of the HIETexas standards, services and policies agreed to by the Participants pursuant to this Agreement. This disclaimer is not intended to diminish or limit in any way the other representations and warranties that the Participant is making in this Agreement. It is intended to recognize that the overall performance of the HIETexas standards, services and policies agreed to by the Participants is beyond the power of any individual Participant to control.

18. **Liability.**

18.01. **Participant Liability**. As between Participants to this Agreement: Each Participant shall be responsible for its acts and omissions and not for the acts or omissions of any other Participant. In circumstances involving harm to other Participants caused by the acts or omissions of individuals who: (i) Transact Message Content or Confidential Participant Information through the Participant; (ii) improperly and without permission access a Participant's system whether directly or indirectly, lawfully or unlawfully; or (iii) use the digital credentials of a Participant or Participant User to access Message Content or Confidential Participant Information, each Participant shall be responsible for such harm to the extent that the individual's access was caused by the Participant's breach of the Agreement or its negligent conduct for which there is a civil remedy under Applicable Law. Notwithstanding any provision in this Agreement to the contrary, Participant shall not be liable for any act or omission if a cause of action for such act or omission is otherwise prohibited by Applicable Law. This section shall not be construed as a hold harmless or indemnification provision.

18.02. **Effect of Agreement**. Except as provided in Section 17.06 (No Warranties), Section 18.03 (THSA Liability) and Article 22 (Dispute Resolution), nothing in this Agreement shall be construed to restrict a Participant's right to pursue all remedies available under law for damages or other relief arising from acts or omissions of other Participants related to this Agreement, or to limit any rights, immunities or defenses to which a Participant or Participant User may be entitled under Applicable Law.

19. **Term, Suspension and Termination**.

19.01. **Term**. The initial term of this Agreement shall be for a period of one year commencing on the Effective Date. Upon the expiration of the initial term, this Agreement shall automatically renew for successive one-year terms unless terminated pursuant to this Section 19.

19.02. **Suspension or Termination by Participant**.

a. A Participant may voluntarily suspend its own right to Transact Message Content by informing the THSA and other Participants of its voluntary suspension in accordance with the Operating Policies and Procedures. Once a Participant has properly informed the THSA and other Participants of its voluntary suspension, neither the Participant, nor its Participant Users, shall Transact Message Content until the voluntary suspension has ended and the Participant has informed the THSA and other Participants that the suspension has ended in accordance with the Operating Policies and Procedures. During the period of the voluntary suspension, the Participant's inability to Transact Message Content and comply with those terms of this Agreement that require Transaction of Message Content shall not be deemed a breach of this Agreement. Any voluntary suspension shall be for no longer than ten (10) consecutive calendar days or for more than forty (40) calendar days during any twelve (12) month period, unless a longer period is agreed to by the THSA.

b. A Participant may terminate its own right to Transact Message Content by terminating this Agreement, with or without cause, by giving the THSA at least five (5) business days prior written Notice. Once proper Notice is given, Participant must cease to Transact Message Content and verify that it has done so, and the THSA shall provide Notice of such reported termination to the remaining Participants.

19.03. **Suspension by THSA.** Upon the THSA completing a preliminary investigation and determining that there is a substantial likelihood that a Participant's acts or omissions create an immediate threat or will cause irreparable harm to another party including, but not limited to, a Participant; a Participant User; the integrity or operation of the Performance and Service Specifications; or an individual whose Message Content is Transacted using the Performance and Service Specifications; the

Participants hereby grant to the THSA the power to require the Participant to summarily suspend, to the extent necessary to address the threat posed by the Participant, the Participant's use of the HIETexas, pending the submission and approval of a corrective action plan, as provided in this Section. Upon suspension, Participant will immediately stop Transacting Message Content on the HIETexas, and within twelve (12) hours of suspending a Participant's right to Transact Message Content, THSA shall (i) provide Notice of such suspension to all Participants; and (ii) provide to the suspended Participant a written summary of the reasons for the suspension. The Participant shall use reasonable efforts to respond to the suspension notice with a detailed plan of correction or an objection to the suspension within three (3) business days or, if such submission is not reasonably feasible within three (3) business days, then at the earliest practicable time. If the Participant submits a plan of correction, the THSA shall, within five (5) business days, review and either accept or reject the plan of correction. If the plan of correction is accepted, the THSA shall, upon completion of the plan of correction, provide Notice to all Participants of such reinstatement. If the plan of correction is rejected, the Participant's suspension will continue, during which time the THSA and the Participant shall work in good faith to develop a plan of correction that is acceptable to both the Participant and the THSA. At any time after the THSA rejects a Participant's plan of correction, either the Participant or the THSA may submit a Dispute to the Dispute Resolution Process described in Section 21. If the THSA and the Participant cannot reach agreement on a plan of correction through the Dispute Resolution Process, the THSA may terminate the Participant in accordance with Section 19.04.

19.04. **Termination by THSA**. The Participants hereby grant to the THSA the power to terminate a Participant's right to Transact Message Content as follows:

a. After taking a suspension action in accordance with Section 19.03 when there is a substantial likelihood that the Participant's acts or omissions create an immediate threat or will cause irreparable harm to another party including, but not limited to, a Participant, a Participant User, integrity or operation of the Performance and Service Specifications, or an individual whose Message Content is Transacted using the Performance and Service Specifications; or

b. In the event a Participant is in material default of the performance of a duty or obligation imposed upon it by this Agreement and such default has not been substantially cured within thirty (30) calendar days following receipt by the defaulting Participant of written Notice thereof from the THSA.

A Participant who is terminated in accordance with this Section may appeal such revocation through the Dispute Resolution Process. However, during the pendency of any such appeal, Participant agrees that it shall cease or continue to cease, as applicable, the Transacting of Health Data at the discretion of the THSA.

19.05. **Effect of Termination.** Upon any termination of this Agreement for any reason, the terminated party shall cease to be a Participant and thereupon and thereafter neither that party nor its Participant Users shall have any rights to Transact Message Content

with other Participants (unless such Participant Users have an independent right to Transact Message Content through another Participant). The THSA shall provide Notice of such revocation to the remaining Participants. In the event that any Participant(s) is terminated, this Agreement will remain in full force and effect with respect to all other Participants. Certain provisions of this Agreement survive termination, as more fully described in Section 23.05 (Survival Provisions).

19.06. **Confidential Participant Information**. Participant will not provide the THSA with any Confidential Participant Information pursuant to this Agreement. In the event that it is determined that the receipt of Confidential Participant Information is needed in order for the THSA to exercise its authority pursuant to this Section, then Participant and THSA will enter into a standard non-disclosure agreement for such purpose.

19.07. **Disposition of Message Content on Termination**. At the time of termination, Recipient may, at its election, retain Message Content on Recipient's System in accordance with the Recipient's document and data retention policies and procedures, Applicable Law, and the terms and conditions of this Agreement, including Section 5.02.

19.08. **Digital Credentials.** Notwithstanding anything to the foregoing, in the event that the THSA, or the eHealth Exchange, as applicable, gains the ability to revoke a Participant's Digital Credentials, Participant acknowledges and agrees that THSA or the eHealth Exchange shall have the un-revocable and absolute right to do so in the event of Suspension or Termination of the Participant in accordance with the THSA's policies or the eHealth Exchange's policies as applicable.

19.09. **Injunctive Relief.** Notwithstanding anything to the foregoing, including the dispute resolution process, nothing in this Agreement, including this Section 19, shall be construed to restrict the THSA from approaching any appropriate court or authority in any relevant jurisdiction for the purposes of obtaining equitable and injunctive relief on behalf of itself or any providers and consumers that may be effected by Participant's continuing to Transact Message Content despite the THSA having notified Participant that it is required to either suspend or terminate its ability to do so. This Section shall survive termination of this Agreement.

20. **Cooperation**. Each Participant understands and acknowledges that numerous activities with respect to this Agreement shall likely involve another Participant's employees, agents, and third party contractors, vendors, or consultants. To the extent not legally prohibited, each Participant shall: (a) cooperate fully with the THSA, each other Participant, and any such third parties with respect to such activities as they relate to this Agreement; (b) provide such information to the THSA, each other Participant, or such third parties as they may reasonably request for purposes of performing activities related to this Agreement; (c) devote such time as may reasonably be requested by the THSA to review information, meet with, respond to, and advise the THSA or other Participants with respect to activities as they relate to this Agreement; (d) provide such reasonable assistance as may be requested by the THSA when performing activities as they relate to this Agreement; and (e) subject to a

Participant's right to restrict or condition its cooperation or disclosure of information in the interest of preserving privileges in any foreseeable dispute or litigation or protecting a Participant's Confidential Participant Information, provide information and assistance to the THSA or other Participants in the investigation of Adverse Security Events and Disputes. In no case shall a Participant be required to disclose PHI in violation of Applicable Law. In seeking another Participant's cooperation, each Participant shall make all reasonable efforts to accommodate the other Participant's schedules and reasonable operational concerns. A Participant shall promptly report, in writing, to any other Participant and the THSA, any problems or issues that arise in working with the other Participant's employees, agents, or subcontractors that threaten to delay or otherwise adversely impact a Participant's ability to fulfill its responsibilities under this Agreement. This writing shall set forth in detail and with clarity the problems that the Participant has identified.

21. **Dispute Resolution**.

21.01. **General**. The Participants acknowledge that it may be in their best interest to resolve Disputes through an alternative dispute resolution process rather than through civil litigation. The Participants have reached this conclusion based upon the fact that the legal and factual issues involved in this Agreement are unique, novel, and complex and limited case law exists which addresses the legal issues that could arise from this Agreement. Therefore, the Participants shall submit Disputes related to this Agreement to the non-binding Dispute Resolution Process attached hereto as Attachment 3 and incorporated herein. Except in accordance with Section 21.02(a), if a Participant refuses to participate in the Dispute Resolution Process, such refusal shall constitute a material breach of this Agreement and may be grounds for termination in accordance with Section 19.04(b).

21.02. **Immediate Injunctive Relief**.

a. Notwithstanding Section 21.01, a Participant may be relieved of its obligation to participate in the Dispute Resolution Process if such Participant (i) believes that the THSA or another Participant's acts or omissions create an immediate threat to the confidentiality, privacy or security of Message Content or will cause irreparable harm to another party (Participant, Participant User, the integrity or operation of the Performance and Service Specifications, or consumer) and (ii) pursues immediate injunctive relief against such other Participant in a court of competent jurisdiction. The Participant pursuing immediate injunctive relief must provide a Notification to the THSA of such action within 24 hours of filing for the injunctive relief and of the result of the action within 24 hours of learning of same.

b. If the injunctive relief sought in Section 21.02(a) is not granted and the Participant seeking such relief chooses to pursue the Dispute, the Participants must then submit to the Dispute Resolution Process in accordance with Section 21.01.

21.03. **Activities during Dispute Resolution Process**. Pending resolution of any Dispute under this Agreement, the Participants agree to fulfill their responsibilities in accordance with this Agreement, unless the Participant voluntarily suspends its right to Transact Message Content in accordance with Section 19.02(a), is suspended in accordance with Section 19.03, or exercises its right to cease Transacting Message Content in accordance with Section 12.01(b).

21.04. **Implementation of Agreed Upon Resolution**. If, at any point during the Dispute Resolution Process, all of the Participants to the Dispute accept a proposed resolution of the Dispute, the Participants agree to implement the terms of the resolution in the agreed upon timeframe.

21.05. **Reservation of Rights**. If, following the Dispute Resolution Process, in the opinion of any involved Participant, the mandatory Dispute Resolution Process failed to adequately resolve the Dispute, the Participant(s) may pursue any remedies available to it in a court of competent jurisdiction.

22. **Notices**. All Notices to be made under this Agreement shall be given in writing to the appropriate Participant's representative at the address listed on the THSA's website, and shall be deemed given: (i) upon delivery, if personally delivered; (ii) upon the date indicated on the return receipt, when sent by the United States Postal Service Certified Mail, return receipt requested; and (iii) if by electronic mail, facsimile telecommunication or other form of electronic transmission, upon receipt when the Notice is directed to a facsimile telecommunication number or electronic mail address listed on the THSA website and the sending facsimile machine or electronic mail address receives confirmation of receipt by the receiving facsimile machine or electronic mail address. It is Participant's responsibility to ensure that the contact information on the THSA website for Participant is current.

23. **Miscellaneous/General**.

23.01. **Governing Law**. In the event of a Dispute between or among the Participants arising out of this Agreement, Texas law shall govern, without regard to its conflict of law provisions.

23.02. **Amendment**. This Agreement may be amended by agreement of at least two-thirds of the Non-Governmental Participants and at least two-thirds of the Governmental Participants. However, if the change is required for the THSA or Participants to comply with Applicable Law, the THSA may implement the change with approval of at least a majority of Non-Governmental Participants and at least a majority of Governmental Participants and within a time period the THSA determines is appropriate under the circumstances. All Participants shall be required to sign an amendment adopted in accordance with the provisions of this Section or terminate participation in accordance with Section 19.02.

23.03. **New Participants**. Upon the THSA's acceptance of a New Participant, the THSA shall have the New Participant execute a Joinder Agreement, the form of which is attached hereto as Attachment 4. The Participants agree that upon execution of the Joinder Agreement by a duly authorized representative of the THSA, all then-current

Participants shall be deemed to be signatories to the Joinder Agreement with the result being that current Participants and the New Participant are all bound by this Agreement. The New Participant shall not be granted the right to Transact Message Content until both it and the THSA execute the Joinder Agreement.

23.04. **Assignment**. No Party shall assign or transfer this Agreement, or any part thereof, without the express written consent of the THSA. Any assignment that does not comply with the requirements of this Section 23.04 shall be void and have no binding effect.

23.05. **Survival**. The provisions of Sections 1, 5.02, 5.03, 14, 15.10, 16, 18, 19.06, 19.07, 20 and 21 shall survive the termination of this Agreement for any reason.

23.06. **Waiver**. No failure or delay by any Participant in exercising its rights under this Agreement shall operate as a waiver of such rights, and no waiver of any right shall constitute a waiver of any prior, concurrent, or subsequent right.

23.07. **Entire Agreement**. This Agreement, together with all Attachments, Participation Agreement between Participants and the THSA, and related Business Associate Agreements, sets forth the entire and only Agreement among and between the THSA and the Participants relative to participation in HIETexas. Any representation, promise, or condition, whether oral or written, not incorporated herein, shall not be binding upon any Participant.

23.08. **Validity of Provisions**. In the event that a court of competent jurisdiction shall hold any Section, or any part or portion of any Section of this Agreement, invalid, void or otherwise unenforceable, each and every remaining Section or part or portion thereof shall remain in full force and effect.

23.09. **Priority.** In the event of any conflict or inconsistency between a provision in the body of this Agreement and any attachment hereto, the terms contained in the body of this Agreement shall prevail.

23.10. **Headings.** The headings throughout this Agreement are for reference purposes only, and the words contained therein may in no way be held to explain, modify, amplify, or aid in the interpretation or construction of meaning of the provisions of this Agreement. All references in this instrument to designated Sections and other subdivisions are to the designated Sections and other subdivisions of this Agreement. The words herein, hereof, hereunder, and other words of similar import refer to this Agreement as a whole and not to any particular Section or other subdivision.

23.11. **Relationship of the Participants.** The Participants are independent contracting entities. Nothing in this Agreement shall be construed to create a partnership, agency relationship, or joint venture among the Parties. Neither the THSA nor any Participant shall have any authority to bind or make commitments on behalf of another Participant for any purpose, nor shall any such Party hold itself out as having such authority. No Participant shall be held liable for the acts or omissions of another Participant.

23.12. **Counterparts.** With respect to the first two Participants to this Agreement, the Effective Date shall be the date on which the second Participant executes this Agreement. For all Participants thereafter, the Effective Date shall be the date that the Participant executes this Agreement or the Joinder Agreement, in accordance with Section 23.03. This Agreement or the Joinder Agreement may be executed in any number of counterparts, each of which shall be deemed an original as against the Participant whose signature appears thereon, but all of which taken together shall constitute but one and the same instrument.

23.13. **Third-Party Beneficiaries**. With the exception of the Participants to this Agreement, there shall exist no right of any person to claim a beneficial interest in this Agreement or any rights occurring by virtue of this Agreement.

23.14. **Force Majeure.** A Participant shall not be deemed in violation of any provision of this Agreement if it is prevented from performing any of its obligations by reason of: (a) severe weather and storms; (b) earthquakes or other disruptive natural occurrences; (c) strikes or other labor unrest; (d) power failures; (e) nuclear or other civil or military emergencies; (f) terrorist attacks; (g) acts of legislative, judicial, executive, or administrative authorities; or (h) any other circumstances that are not within its reasonable control. This Section 23.14 shall not apply to obligations imposed under Applicable Law.

23.15. **Time Periods.** Any of the time periods specified in this Agreement may be changed pursuant to the mutual written consent of the THSA and the affected Participant(s).

This Agreement has been entered into and executed by officials duly authorized to bind their respective parties.

Attachment 1
Operating Policies and Procedures

OPP 1: Participation – Review and Disposition of Applications for Participation

I. Purpose

The Texas Health Services Authority ("THSA") is responsible for supporting Participants who wish to Transact Message Content with other Participants. Among the responsibilities granted to the THSA by the Participants is the right to determine whether to admit new Participants who will be signatories to the Health Information Exchange ("HIE") Texas ("HIETexas") State-Level Trust Agreement (hereinafter "the State-Level Trust Agreement"). To fulfill this responsibility, the THSA will review and act on applications for Participation ("Application(s)") submitted by organizations that wish to become Participants ("Applicants"). This policy outlines a framework for assessing the qualifications, eligibility and readiness of valid legal entities and governmental entities to become Participants.

II. Policy

The THSA, in the exercise of its discretion applying the participation requirements set forth below, will accept Applicants as Participants.

A. General Eligibility Requirements (Administrative)

1. To be accepted as a Participant, an Applicant must meet all of the following administrative criteria, hereinafter referred to as "General Eligibility Requirements":
    a. Be a valid business in good standing or a governmental agency, operating in the Texas;
    b. Meet all solvency and financial responsibility requirements imposed on the Applicant by applicable statutes and regulatory authorities;
    c. Have a governing body that creates trust and consensus on exchange of health information, provides oversight, transparency, and accountability, and protects the interest of the public;
    d. Utilize a system which has been verified as compliant with the Performance and Service Specifications described in the State-Level Trust Agreement;
    e. Have the organizational infrastructure and legal authority (through statutes, regulations, organizational agreements, contracts or binding policies) to comply with the obligations in the State-Level Trust Agreement and to

require its Participant Users to comply with applicable requirements of the State-Level Trust Agreement;

f. Intend to Transact information with other Participants for a Permitted Purpose;

g. Have sufficient financial, technical, and operational resources to support the testing and operation of transactions among Participants;

h. Is not aware of any information that would preclude the Applicant from fully complying with the provisions of the State-Level Trust Agreement; and

i. Submit the completed Application and the signed Joinder Agreement[1] (Attachment 4 of the State-Level Trust Agreement), along with the applicable participation fees.

2. Organizations not meeting the criteria listed in Section A1 (above) will be considered on a case-by-case basis at the discretion of the THSA.

3. General Eligibility Requirements may be amended from time to time, as determined by the THSA. In addition, an Applicant's past activities as a Participant may be considered.

4. While an Applicant's Application must include a signed copy of the Joinder Agreement, such signature does not make the Applicant a party to the State-Level Trust Agreement. The Applicant does not become a party to the State-Level Trust Agreement until the THSA accepts the Applicant as a Participant and duly executes the Applicant's Joinder Agreement. The THSA reserves the right to decline an Applicant participation even if such Applicant signs the Joinder Agreement in the exercise of the THSA's discretion in applying the criteria set forth in this document.

B. Technical Requirements

In addition to the General Eligibility Requirements, to be accepted as a Participant, the Applicant must also satisfy the following Technical Requirements:

1. Has a system implemented in a production-ready environment that complies with the Performance and Service Specifications as set forth in Section 10 of the State-Level Trust Agreement;
2. Successfully complete the required technical testing of Applicant's system in accordance with the THSA Onboarding Plan; and
3. Certify the Applicant is ready to begin exchanging data with other Participants in production through the Applicant's successfully tested system.

[1] The Joinder Agreement (Attachment 4 of the State-Level Trust Agreement) acts as a signatory page to the State-Level Trust Agreement, which establishes the multi-party agreement among all Participants in HIETexas. During the onboarding process, Applicants will also be required to sign a Participation Agreement (not mentioned in these Operational Policies & Procedures), which establishes the individual agreement between the Participant and the THSA.

III. Procedure

The following procedures outline the steps for determining whether an Applicant has satisfied the eligibility requirements to be a Participant. The process for testing and determining whether a system complies with the Performance and Service Specifications is addressed in the THSA onboarding plan.

A. Verify General Eligibility Requirements (Administrative)

1. THSA Responsibilities and Delegation of Rights. The THSA will be responsible for duties and responsibilities including but not limited to: the receipt, processing, and review and disposition of Applications.

2. Application Submission

Applicants shall prepare and submit their Application to the THSA at SLSS@thsa.org or other electronic means as approved by the THSA. The THSA will acknowledge receipt of all Applications within three (3) business days. The Applicant shall contact the THSA to confirm receipt if an electronic confirmation is not received from the THSA within three (3) business days.

The Application supports the verification of eligibility requirements set forth in the Policy Section above. For details regarding the type of information that should be included in the Application, please see the Guidance in Section II(A) above.

3. Readiness Review of the Application

The THSA shall conduct a cursory review of the Applications in a timely manner and determine if the Application is ready for review.

4. Review and Disposition of Application

a. The THSA shall review the Application and determine whether an Applicant meets the General Eligibility Requirements. So long as the Applicant provides timely responses, it is anticipated that this process will usually be completed within sixty (60) calendar days.

b. The THSA may consult with the Applicant to request additional information regarding the Application and proposed services and/or transactions, suggest changes or modifications to the Application including the supporting documentation, request verification of elements of the Application including screen shots, audit log excerpts, metrics or system demonstrations, or make other recommendations the deemed reasonably necessary during the review.

If the Applicant fails, or declines, to respond to the request, provide requested information, or modify its Application within sixty (60) calendar days of the THSA's request, the Application may be considered withdrawn.

If the THSA determines that the Applicant meets the General Eligibility Requirements, the Applicant will be directed to complete requisite testing.

c. If the Application does not meet the General Eligibility Requirements, the Applicant will be notified in writing within sixty (60) calendar days. An Applicant may submit a new Application for future consideration by the THSA after correcting the identified deficiencies.

d. Any Applicant may withdraw its Application at any time prior to approval by the THSA by informing the THSA of such withdrawal.

e. Once the determination for acceptance or rejection of an Application has been made, the Applicant shall be informed in writing by the THSA within sixty (60) calendar days of the decision as well as supporting rationale.

B. Verify Technical Requirements

1. Receipt and Evaluation of Applicant Test Results

a. During consideration of the test results, the THSA may consult with the Applicant, request additional information, notify the Applicant of items that require remediation to comply with the Performance and Service Specifications or suggest changes to the Applicant's implementation of the Performance and Service Specifications.

b. The Applicant shall notify the THSA of its election to remediate or not remediate any non-conformance of its implementation of the Performance and Service Specifications.

c. If the Applicant elects not to remediate any non-conformance, the Application shall be considered to be withdrawn.

d. The THSA may hold an Application pending completion of any needed remediation, changes or modifications as well as any needed follow-up testing to ensure the Applicant is able to meet the Performance and Service Specifications.

C. Determine Participation

1. If the Applicant meets the General Eligibility Requirements and has successfully completed all required testing, the Applicant shall be conditionally accepted as a Participant, subject to the discretion of the THSA.

2. The Applicant's acceptance as a Participant is conditioned on the Applicant's being able to begin exchanging data in production with other Participants within one-hundred-and-twenty (120) calendar days following the date the Applicant was conditionally accepted as a Participant. During that time the following activities will occur:

    a. No more than thirty (30) calendar days before an Applicant is scheduled to be activated to begin exchanging information with Participants in production, the THSA will execute the Joinder Agreement.

    b. THSA will issue the Applicant its Digital Credentials.

    c. The Applicant shall provide the requested information to the THSA to perform technical enrollment of the Participant's services.

    d. THSA shall enroll the Applicant onto HIETexas within seven (7) calendar days of receiving such required information.

    e. At this point the Applicant becomes activated as a Participant. Other Participants will be able to identify the new Participant and begin transacting health information with that new Participant. The THSA will provide a notification to other Participants informing them that a new Participant has been added to HIETexas.

3. If an Applicant is unable to go into production as a Participant within the one-hundred-and-twenty (120) calendar-day timeframe or on another date mutually agreed upon by the THSA and Participant, the Applicant may request an extension.

    a. Extension requests must be made in writing prior to end of the original 120-day period or the expiration of a previous acquired extension and submitted to the THSA. The request shall include the rationale of the extension and the number of days requested.

    b. If the extension request is denied, it shall have the same effect as a rejection.

    c. If the extension request is accepted, it shall result in the extension of the timeframe for the Applicant to identify a specific effective date on which the Applicant's system will be operational, in production and ready to exchange information with other Participants in production.

    d. Applicants may submit multiple extension requests, each of which the THSA will review and disposition.

4. An Applicant's formal acceptance as a Participant takes effect on the date the Applicant's system is operational in a production environment and able to transact Message Content with other Participants and when the Applicant's

Digital Credentials are activated.

D. Examples

The following are several examples that illustrate ways in which the THSA may apply the General Eligibility Requirements. These examples are not intended to describe all possible scenarios.

- **Scenario 1**: An entity that licenses system software to its clients, but has not confirmed it has an agreement with its clients that requires the clients to use the software to transact information only for the purposes allowed by the State-Level Trust Agreement.

  Scenario 1 – Eligibility Implications: The entity is not eligible to be a Participant because the entity does not have the legal authority to require its clients to comply with the applicable requirements of the State-Level Trust Agreement.

- **Scenario 2**: An entity that facilitates the transaction of information among various parties by helping the parties to reach agreement on conduct expectations, but does not provide the software that allows those parties to transact information.

  Scenario 2 – Eligibility Implications: The entity is not eligible to be a Participant because it does not have the technical ability to meet the Performance and Service Specifications and does not conduct exchanges of health information.

- **Scenario 3**: An entity that licenses software to its clients that allows the clients to transact data with other Participants without the oversight of the entity as an intermediary.

  Scenario 3 – Eligibility Implications: The entity is not eligible to be a Participant because the entity is not overseeing and conducting exchanges of health information.

- **Scenario 4**: An entity that licenses software to its clients, acts as its clients' intermediary in the exchange of information with others, and has agreements with its clients that require the clients to use the software in accordance with the terms of the State-Level Trust Agreement.

  Scenario 4 – Eligibility Implications: The entity is eligible to be a Participant.

IV. ***Definitions:***

Applicant: The entity that submits an Application for Participation.

Application for Participation ("Application"): The document that serves as an application to participate in HIETexas.

State-Level Trust Agreement: The agreement entered into by Participants in HIETexas.

THSA Onboarding Plan: The THSA Onboarding Plan defines the process and requirements needed for an HIETexas Applicant to become a Participant.

All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the HIETexas State-Level Trust Agreement.

OPP 2: THSA General Operating Procedure

I. Purpose

The Texas Health Services Authority ("THSA") derives its authority from the State-Level Trust Agreement and Chapter 182, Texas Health and Safety Code. One purpose of the THSA is to enhance trust relationships between the Participants by fulfilling certain responsibilities described in the State-Level Trust Agreement. Participants have recognized that a structure is needed to assure these critical responsibilities are successfully implemented.

The THSA must operate efficiently and effectively to fulfill its many important tasks. This Operating Policy and Procedure describes how representation by the THSA is implemented in accordance with the State-Level Trust Agreement and how the THSA will operate in the performance of its responsibilities.

II. Policy

The THSA facilitates decisions related to its duties described in the State-Level Trust Agreement, oversees strategic, operational, and management issues related to HIETexas, and provides support to the Participants. The THSA will work in a timely fashion to achieve consensus on issues brought before it.

The THSA formed several stakeholder task forces to monitor ongoing developments related to HIE capabilities including data standards, security, and technical architecture, and provide input to the THSA Collaboration Council on common policies and procedures, standards, technical approaches, and shared services. The Board of Directors will consider these common policies and other recommendations developed through this collaborative process and issue Statewide Policy Guidance to Participants as necessary to support a common and consistent technical, privacy, security, and legal framework for HIE in Texas. Guidance developed through this process shall be reviewed on a regular basis.

III. Procedure

A. Purpose of the THSA Collaboration Council

The purpose of the THSA Collaboration Council is to monitor the implementation of HIE within the state and to make recommendations on common policies and procedures, standards, technical approaches, and services to support the necessary statewide HIE infrastructure in Texas.

B. Membership of the THSA Collaboration Council

The THSA Collaboration Council is composed of several members, potentially including, but not limited to:

1. THSA Staff (Collaboration Council Chair);

2. Four (4) HIE Representatives – one state-funded local HIE representative per Regional Extension Center (REC) region to provide input from regional/local HIEs to ensure a coordinated approach to HIE implementation and operations within Texas;
3. State Health Information Technology Coordinator;
4. The Commissioner, or a representative designated by the Commissioner, of the Texas Department of State Health Services;
5. An individual designated by the Texas Association of Health Plans;
6. An individual designated by the Texas Hospital Association;
7. An individual designated by the Texas Medical Association;
8. Four (4) REC representatives – one individual per approved REC;
9. Employer representative – an individual representative of an employer; and
10. Consumer representative – an individual who is a consumer of health care services and has expertise in privacy and security of health information.

Ex-Officio Membership: The following organizations shall designate one member to serve as an ex-officio member of the Collaboration Council:

1. One representative from all other state-funded HIE Participants that are not a member of the Collaboration Council;
2. Texas Association of Community Health Centers;
3. Texas Council of Community Mental Health & Mental Retardation Clinics;
4. Texas e-Health Alliance;
5. Texas Pharmacy Association; and
6. Any other member the THSA Chief Executive Officer designates.

C. Notice of Meetings

The THSA Collaboration Council shall maintain a regular meeting schedule, including date, time and location, and provide as much advance notice as possible to task force members. The THSA will publish a calendar of upcoming meetings on its web site. Other meetings may also be scheduled on an ad hoc basis, providing as much advanced notice as possible.

D. Documentation of Meetings

The THSA shall maintain meeting notes that summarize the discussion and decisions at each of its meetings. After approval by the THSA, meeting notes may be posted publicly. To the extent that any item is approved by the THSA and needs to be communicated to third parties, such item shall be communicated in a separate email, memorandum, or other transmittal as deemed appropriate by the THSA.

OPP 3: Participation – Changes, Suspension, and Termination

I. Purpose

The THSA is responsible for developing, implementing, and overseeing the operations of HIETexas. The fulfillment of these responsibilities involves making changes with regard to the Transaction Patterns supported by a Participant as well as suspension and termination of Participants based upon a Participant's request or upon action of the THSA.

II. Policy

This Policy outlines a framework for accepting and reviewing requests by Participants to make changes with regard to the Transaction Patterns they support, as well as processes and procedures for suspension and termination of a Participant, whether initiated by the Participant or by the THSA.

A. Changes to Transaction Patterns

A Participant may notify the THSA of the Participant's plan to add, modify, or terminate a Transaction Pattern ("Service Change"). The THSA will strive to comply with all Service Change requests.

B. Suspension

1. *Voluntarily by the Participant.*

   Pursuant to Section 19.02(a) of the State-Level Trust Agreement, a Participant may voluntarily suspend its right to Transact Message Content.

2. *With Cause by the THSA.*

   Pursuant to Section 19.03 of the State-Level Trust Agreement, the THSA may suspend a Participant's use of the HIETexas.

3. *Reinstatement by the THSA.*

   Pursuant to Section 19.03 of the State-Level Trust Agreement, after a period of suspension and upon successful completion of the Participant's corrective action plan or other measures directed by the THSA, the THSA shall reinstate a Participant's Digital Credentials, if applicable, and provide notice to all Participants of such reinstatement.

C. Termination

1. *Voluntarily by the Participant.*

Pursuant to Section 19.02(b) of the State-Level Trust Agreement, a Participant may voluntarily terminate its participation.

2. *With Cause by the THSA.*

Pursuant to Section 19.04 of the State-Level Trust Agreement, the THSA may terminate a Participant from participating in HIETexas.

III. Procedure:

A. Service Changes

1. All requests for Service Changes by a Participant shall be directed to the THSA in writing. The THSA may summarily approve a Service Change, further consult with other Members of the THSA, or call a special meeting of the THSA to discuss the Service Change request. The THSA shall communicate all approved Service Changes to each Participant. The THSA shall take all appropriate technical actions necessary to carry out the Service Change.

2. Where a Service Change request involves the addition or modification of a Transaction Pattern, the THSA shall request that the Participant complete all technical testing in accordance with the THSA onboarding plan to assess compliance of the new or modified Transaction Pattern with the applicable Performance and Service Specifications.

3. If the Participant has successfully completed all technical testing in accordance with the Validation Plan, the following activities will occur:

- The THSA shall coordinate with the Participant regarding the specific date on which the Participant's new, modified, or deleted Transaction Pattern will take effect in production.

- The Participant shall provide THSA the required information to provision the Particpant's new, modified, or deleted services in the HIETexas operational environment. THSA will confirm that the information supplied is accurate by testing the information provided.

- If the information supplied is accurate and the tests are successful, THSA shall provision or decommission the Particpant's new, modified, or deleted services in the HIETexas operational environment.

- The THSA shall notify all other Participants of the new, modified, or deleted services.

4. Where the Service Change request involves the termination of the Participant's ability to respond to Messages that seek Message Content for Treatment, the THSA shall take all appropriate technical actions to ensure that the Participant cannot request Message Content for Treatment.

B. Suspension

1. *Voluntarily by the Participant.*

Service Level Interruptions

Participants will experience temporary service level interruptions from time to time. These service level interruptions may be planned or unplanned. A service level interruption will result in a Participant having to temporarily cease exchanging Message Content with all other Participants. To ensure that all Participants are aware of a service level interruption, the Participant experiencing the service level interruption will send a written notice to the THSA of the interruption prior to the interruption, if planned, or as soon as reasonably practicable, but in no case longer than three (3) business days, after the interruption begins if unplanned. THSA will notify all other Participants of the interruption. Because a service level interruption does not involve the termination of a Participant's Digital Credentials, the Participant will be responsible for taking all technical actions necessary to carry out a service level interruption. During a service level interruption, the Participant will continue to be responsible for complying with the terms of the State-Level Trust Agreement.

Voluntary Suspension

If, at any point, a Participant decides that it requires a temporary suspension from participation and its responsibility for complying with the State-Level Trust Agreement, it shall send a written notice to the THSA. The Participant must give notice of its need for a temporary voluntary suspension at least twenty-four (24) hours prior to commencing its voluntary suspension.[2] The notice will specify the reason for, the commencement date of, and the duration of the voluntary suspension.

If the voluntary suspension will last fewer than ten (10) calendar days and will not cause the Participant to exceed forty (40) calendar days of voluntary suspension in the twelve (12) months preceding the start of the planned suspension, the THSA will assume that it is for a valid purpose and will take appropriate technical actions necessary to carry out the voluntary suspension. THSA will notify all other Participants of such voluntary suspension.

If the duration of the voluntary suspension will exceed ten (10) calendar days or cause the Participant to exceed forty (40) calendar days of voluntary suspension in the twelve (12)

[2] A Participant may choose to undergo a service level interruption during this 24-hour period.

months preceding the start of the planned suspension, the THSA will review and decide whether to approve the voluntary suspension. Upon receipt of a notice of such a voluntary suspension, the THSA shall evaluate and make a determination on the suspension request. The THSA shall determine whether the request is for a valid purpose and whether the duration is acceptable. The THSA shall communicate its determinations to the Participant in writing with an explanation of its decision. If the suspension is approved, the THSA shall notify all other Participants of the suspension and take all appropriate technical actions necessary to carry out the voluntary suspension.

If the THSA determines that the request for voluntary suspension is not for a valid purpose or that the duration of the voluntary suspension is unacceptable, the THSA will meet with the requesting Participant to discuss the determination. The THSA and the Participant will work together in good faith to reach an acceptable resolution. If they cannot reach a resolution, they will submit the Dispute to the Dispute Resolution Process.

2. *With Cause by the THSA.*

Upon receipt of a complaint, report or other information, including but not limited to failure to report a service level interruption within a reasonable period of time, that causes the THSA to question whether a Participant's acts or omissions are creating an immediate threat or will cause irreparable harm to another party, the State-Level Trust Agreement gives the THSA the legal authority to investigate the complaint, report or other information and determine whether such Participant should be suspended. Any suspensions imposed under this Policy shall remain in effect until the Participant is reinstated or terminated in accordance with the State-Level Trust Agreement and this Policy.

THSA will immediately take appropriate technical actions necessary to carry out the suspension, which may include but is not limited to, suspension of the Participant's Digital Credentials. As soon as reasonably practicable after suspending a Participant, but in no case longer than twelve (12) hours, the THSA will provide the suspended Participant with a written summary of the reasons for the suspension and notify all other Participants of the suspension.

The suspended Participant will provide the THSA with a written plan of correction or an objection to the suspension within three (3) business days of its receipt of the written summary of the suspension, or if such response is not reasonably feasible within the three (3) day timeframe, then at the earliest practicable time.

Objections and Plan of Correction

Any objection by the Participant shall be specified in writing stating the reason why the suspension is inappropriate. A plan of correction shall be included and shall describe the steps that the Participant is taking to address, mitigate and remediate the issue(s) that caused the THSA to determine that a summary suspension was appropriate and include a timeframe for such actions. The THSA will review a suspended Participant's plan of correction or

objection within ten (10) calendar days of receiving same from the Participant; determine whether to accept or reject the objection or the plan of correction or affirm the suspension; and communicate such decision to the suspended Participant in writing with an explanation of its decision.

If the THSA rejects the plan of correction, it will work in good faith with the suspended Participant to develop a mutually acceptable plan of correction. If the THSA and the suspended Participant cannot reach agreement on the content of the plan of correction or on the reasons supporting the suspension itself, the THSA may submit the Dispute to the Dispute Resolution Process or terminate the Participant.

C. Reinstatement

1. *Post-Participant Voluntary Suspension*

The Participant's request for a voluntary suspension will state the commencement date and the duration of the suspension. The Participant will have the ability to seek an extension of its voluntary suspension should one be necessary. If the extension will cause the suspension to exceed ten (10) calendar days or cause the Participant to exceed forty (40) calendar days of voluntary suspension in the twelve (12) months preceding the start of the planned suspension, the Participant shall provide additional justification for the extension request. The THSA will review, evaluate and make a written determination on the extension request and provide it to the Participant.

Either on the date indicated by the Participant in the voluntary suspension or extension request or at an earlier time if requested by the Participant, the THSA shall take appropriate technical actions necessary to reinstate the Participant's ability to participate in HIETexas.

2. *Post-Suspension with Cause by the THSA.*

Where a Participant's ability to participate in HIETexas has been suspended by the THSA with cause, the Participant shall provide evidence to the THSA of the Participant's fulfillment of the obligations of its plan of correction. The THSA will review such evidence within three (3) business days of receiving it from the Participant.

If the THSA is not satisfied that the Participant has met its obligations under its plan of correction, the THSA will inform the Participant of the deficiencies. The Participant may submit additional evidence that addresses such deficiencies or the Participant may terminate its participation.

When the THSA is satisfied that the evidence presented indicates that the Participant has fulfilled its obligations under the plan of correction, the THSA will take appropriate technical actions necessary to reinstate the Participant's ability to participate.

D. Termination

1. *Voluntarily by the Participant.*

   All requests for termination by a Participant shall be directed to the THSA in writing at least five (5) business days prior to the requested termination date. The THSA will take appropriate technical actions necessary to carry out the termination including, but not limited to, termination or suspension of the Participant's Digital Credentials. The THSA will notify all other Participants of the termination and remove the Participant from the registry and published lists of HIETexas Participants.

2. *With Cause by the THSA.*

   (a) *Immediate Threat Upon Suspension Investigation.* If, after further investigation following its suspension for cause of a Participant in accordance with Section B.2 of this Policy, the THSA believes that there is a substantial likelihood that the Participant's acts or omissions will continue to create an immediate threat or will cause irreparable harm to another party, the THSA may terminate the Participant. In the event the Participant is terminated, the THSA shall notify the Participant of the termination along with the Participant's right to appeal the determination through the Dispute Resolution Process (*see* State-Level Trust Agreement, Section 21).

   (b) *Complaint of Material Default.* If based on a complaint, report, or other information the THSA finds that a Participant is in material default of the performance of a duty or obligation imposed on the Participant by the State-Level Trust Agreement, it shall notify the Participant, in writing, with a written summary of the basis of the default and the actions required to cure the default ("Cure Notice"). Actions to cure the default must be taken with thirty (30) calendar days following Participant's receipt of the Cure Notice or such other time period as agreed upon by the THSA and the Participant (the "Cure Period").

   Material defaults include, but are not limited to, failure to comply with:

   (i) Any privacy, security or confidentiality obligations in the State-Level Trust Agreement;

   (ii) Any expectations or duties of a Participant, as provided for in the State-Level Trust Agreement; and

   (iii) Any breach of the representations and warranties in the State-Level Trust Agreement.

   During the Cure Period, the THSA may suspend the Participant in accordance with Section B.2 of this Policy or continue any existing suspension. The THSA will consider all relevant information submitted by the Participant and actions taken by the Participant during the Cure Period in response to the Cure Notice. If the

Participant does not substantially cure its material default within the Cure Period, the THSA may terminate the Participant. In the event that the Participant is terminated, the THSA shall (1) issue a final written notice of termination; (2) take appropriate technical actions necessary to carry out the termination including, but not limited to, termination of the Participant's Digital Credentials; and (3) notify all other Participants of the termination.

VI. Definitions:

Service Registry shall mean a directory of Participants that is used by Participants to find and Transact Message Content among Participants.

All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the State-Level Trust Agreement.

OPP 4: State-Level Trust Agreement and Amendment Process

I. Purpose

The THSA is responsible for managing amendments to the State-Level Trust Agreement. The purpose of this policy is to set forth the process by which the THSA will fulfill this responsibility.

II. Policy

The THSA shall establish and maintain a process for amending the State-Level Trust Agreement that is consistent with Section 23.02 of the State-Level Trust Agreement. An amendment to the State-Level Trust Agreement shall be effective only if approved as provided in this policy and Section 23.02 of the State-Level Trust Agreement.

III. Procedure:

A. Retention and Dissemination of the State-Level Trust Agreement

The THSA shall maintain the State-Level Trust Agreement on its web site. The THSA shall maintain all original, or valid electronic, executed copies of the State-Level Trust Agreement. In addition, the THSA shall also maintain a list of the current Participants on THSA.org.

The current version of the State-Level Trust Agreement as well as originals of all previous versions shall be maintained for the duration of their usefulness as determined by the THSA.

B. Submission of Proposed Amendments to the State-Level Trust Agreement

The THSA, any Participant, or any other stakeholder that the THSA deems appropriate may submit in writing to the THSA a request for an amendment to the State-Level Trust Agreement. Additionally, the THSA may, at its discretion, solicit requests for amendments to the State-Level Trust Agreement from all Participants and other interested stakeholders. All requests for proposed amendments shall adhere to the following format:

State-Level Trust Agreement Proposed Amendment			
Participant:		**Contact Name:**	
Email Address:		**Phone Number:**	
SLTA Page #:		**SLTA Section #:**	
Suggested Amendment:			

State-Level Trust Agreement Proposed Amendment	
Rationale for Amendment:	

C. Consideration of Proposed Amendments to the State-Level Trust Agreement

The THSA will evaluate the proposal, as appropriate. After considering the request, the THSA will determine how to disposition the request and will communicate this determination to the requestor in a written explanation.

If, after considering the request, the THSA determines that the request requires further consideration, it will forward the request to a task group designated by the THSA to review the request and make a recommendation for action to the THSA.

If the task group's recommendation is that the State-Level Trust Agreement should not be amended and the THSA approves such a recommendation, the THSA will inform the requestor of its determination in a written explanation.

If the task group's recommendation is to amend the State-Level Trust Agreement and the THSA approves such a recommendation, the THSA will identify the timeframe in which it will seek Participant approval of the recommended amendment, either individually or bundled with other scheduled amendments, and when the amendment should be circulated for Participant signature.

When the THSA informs the Participants of its recommendations for amendments to the State-Level Trust Agreement and seeks Participant approval of such amendments, the THSA will provide Participants with the following information:

- A copy of the proposed amendment to the State-Level Trust Agreement;
- A reasonably comprehensive statement as to the reasons for the proposed amendment and any foreseeable impact of the change;
- A statement regarding whether the proposed amendment is necessary in order for HIETexas, the THSA, or Participants to comply with Applicable Law; and
- A projected effective date for the proposed amendment.

D. Approval of Proposed Amendments to the State-Level Trust Agreement

Amendments to the State-Level Trust Agreement must be approved by the Participants in accordance with Section 23.02 of the State-Level Trust Agreement. The requirements of that section are explained below.

For proposed amendments to the State-Level Trust Agreement that are not required for HIETexas, the THSA, or Participants to comply with Applicable Law, at least two-thirds of the Participants must

approve the amendment in order for it to be approved.

For proposed amendments to the State-Level Trust Agreement that are required for HIETexas, the THSA, or Participants to comply with Applicable Law, at least a majority of the Participants must approve the amendment in order for it to be approved.

The THSA will provide all Participants with notice of the approval of a proposed amendment at least thirty (30) calendar days prior to the effective date of the amendment. Within fifteen (15) calendar days of receiving notice of the amendment, a Participant may request that the THSA delay the effective date of the amendment based on unforeseen complications or other good cause. The THSA will meet to evaluate and respond to the request in writing within seven (7) calendar days.

Once an amendment is approved by the Participants, the THSA will distribute or make the amendment available for execution by all Participants, who must sign the amendment to the State-Level Trust Agreement prior to the effective date of the amendment or terminate their participation in accordance with the State-Level Trust Agreement and Operating Policy and Procedure # 3.

OPP 5: HIETexas Change Process

I. Purpose

The Texas Health Services Authority ("THSA") has responsibility for developing, maintaining, repealing, amending and retaining Operating Policies and Procedures ("OPPs"). The purpose of this policy is to set forth the procedure by which the THSA will fulfill these responsibilities.

II. Policy

The THSA shall establish and maintain reasonable OPPs. OPPs are those documents that describe the management, operation, and participation in HIETexas. As may become necessary for the proper functioning of HIETexas, the THSA may establish a new OPP, or it may amend, repeal, and/or replace any existing OPPs, consistent with this policy and the State-Level Trust Agreement.

III. Procedure:

A. Retention, Maintenance and Dissemination of Operating Policies and Procedures

All OPPs shall be maintained in an accessible electronic and printable format. The THSA shall maintain the OPPs in a location that is accessible to all Participants, the THSA, and any other stakeholders that the THSA determines require access.

All current OPPs as well as originals of all amended, repealed and replaced OPPs shall be maintained for the duration of their usefulness as determined by the THSA.

B. Submission of Proposed New, Amended, Repealed, or Replaced Operating Policies and Procedures

Any Participant may submit in writing to the THSA a request for the development of a new OPP, or a request for the amendment or repeal of an existing OPP. The THSA may also bring forth any concern or question regarding OPPs. All such requests shall be considered on an annual basis, to be determined at the discretion of the THSA.

C. Consideration of Proposed New, Amended, Repealed, or Replaced Operating Policies and Procedures

1. Except as otherwise provided in the State-Level Trust Agreement, the THSA will consider any requests on an annual basis, to be determined at the discretion of the THSA. The THSA will:
    a. Prioritize requests;
    b. Consider the merits of the request, as well as the impact to Participants, Participant Users and Individuals; and
    c. Communicate actions taken with requestor.

2. Participant Comment Period. Prior to approving any new, amended, repealed or replaced OPP, the THSA shall solicit and consider comments from the Participants on the new, amended, repealed or replaced OPP.

   To promote openness and transparency, the THSA may post proposed changes to the OPPs to a publicly accessible location.

3. Objection Period. Following the THSA's approval of the new, amended, repealed or replaced OPP, the Participants shall be given thirty (30) calendar days to review the approved OPP and register an objection if the Participant believes the new, amended, repealed or replaced OPP will have a significant adverse operational or financial impact on the Participant. Such objection shall be submitted to the THSA and contain a summary of the Participant's reasons for the objection. The THSA shall respond to the requestor within thirty (30) calendar days of receiving such objection.

D. Implementation

The THSA shall provide notice of new, amended, repealed or replaced OPPs at least thirty (30) calendar days prior to the effective date of such new, amended, repealed or replaced OPP. This thirty (30) calendar-day period may run concurrently with the thirty (30) calendar-day objection period.

OPP 6: HIETexas Information Handling

I. Purpose

In fulfilling its obligations under the State-Level Trust Agreement, the Texas Health Services Authority ("THSA") may request and receive information from Applicants and Participants. To the extent that such information is labeled by an Applicant or Participant as "Confidential Participant Information," it will be treated as such by the THSA, unless required to disclose information as described in Section (III)(6)(c). This policy sets forth the procedure by which the THSA will handle Confidential Participant Information.

II. Policy

Subject to *Section (III)(6)(c),* the THSA is obligated to hold all Confidential Participant Information in confidence and agrees that the THSA shall not disclose to any person or entity, nor use for the THSA's business or benefit, any information obtained in connection with the THSA's performance of duties. The THSA is obligated to maintain the confidentiality of Confidential Participant Information, except as necessary to fulfill the obligations of the State-Level Trust Agreement and *Section (III)(6)(c)*.

Any support staff and advisors, who the THSA provides access to Confidential Participant Information or in support of HIETexas, are obligated to maintain the confidentiality of such Confidential Participant Information post and during his/her employment by, or contractual relationship with the THSA.

III. Procedure

1. *Request for Information*: In the exercise of its obligations under the State-Level Trust Agreement, the THSA may request information from Participants and Applicants for the following reasons:
    a. Determining whether to admit new Participants to HIETexas;
    b. Suspending or terminating Participants in accordance with the State-Level Trust Agreement;
    c. Receiving reports of Adverse Security Events and acting upon such reports in accordance with the State-Level Trust Agreement;
    d. Resolving Disputes between Participants in accordance with the State-Level Trust Agreement;
    f. Determining materiality of proposed new, or changes to existing, Performance and Service Specifications in accordance with the State-Level Trust Agreement;
    g. Developing and amending the THSA Operating Policies and Procedures in accordance with the State-Level Trust Agreement;
    h. Managing the amendment of the State-Level Trust Agreement in accordance with the State-Level Trust Agreement; and

i. Fulfilling all other responsibilities delegated by the Participants to the THSA as set forth in the State-Level Trust Agreement.

2. *Identification of Confidential Participation Information:* Upon receipt of information from Applicants or Participants, the THSA will determine whether the information bears a label that indicates that it is Confidential Participant Information. Such labels do not have to say "Confidential Participant Information," but must indicate the confidential nature of the information. Acceptable labels include, but are not limited to, "confidential," "proprietary," and "do not disclose." Regardless of its label, any information received by the THSA may still be subject to the Public Information Act, as described in Section (III)(6)(c), and in that context will be deemed confidential only if the information meets an exception under the Public Information Act.

3. *Participant Requests for Additional Restrictions.* Participants are permitted to request restrictions on the disclosure of their Confidential Participant Information beyond those restrictions provided in the State-Level Trust Agreement and this Operating Policy and Procedure. The THSA will review all such requests and, in its sole discretion, will determine whether to approve such requests. The THSA will notify the Participant of its decision regarding the request.

4. *Storage of Confidential Information:*

   a. Confidential Participant Information that is received by the THSA in either electronic form or hard copy shall be properly secured to minimize risks to unauthorized access. Access to the systems and storage locations designated for Confidential Participant Information will be limited to the THSA and such support staff and advisors who require access to such information for performance of their work, as determined by the THSA. On a routine basis, but no less frequently than every six (6) months, the THSA will review a list of those who have access to the systems designated for Confidential Participant Information and confirm the accuracy of the list.

   b. The electronic file name for any Confidential Participant Information will indicate that it is Confidential Participant Information. Electronic files will be renamed, if necessary, by the THSA, when stored on the systems designated for Confidential Participant Information.

   c. The THSA shall not store Confidential Participant Information on their personal or business computers or in their own files.

   d. Confidential Participant Information may be submitted electronically per methods approved by the THSA.

5. *Retention:* Confidential Participant Information will be retained for the duration of its usefulness in accordance with the THSA Records Retention Policy, which is available for review on the THSA's website; as required by contract, law, and/or business use; or, until the THSA's duties are assigned to any successor organization with responsibility for oversight of the operation and support of HIETexas.

6. *Use and Disclosure Limitations of Confidential Participant Information:*

    a. Confidential Participant Information will be used only by the THSA to fulfill the THSA's obligations under the State-Level Trust Agreement. The THSA will not disclose to any person or entity, nor use any information obtained in connection with the THSA's performance of its duties under the State-Level Trust Agreement.
    b. To the extent that the THSA shares Confidential Participant Information with third parties that support the operations of the THSA (e.g. consultants, legal counsel, advisors, support staff), the THSA will ensure that these third parties are contractually bound to the same (or substantially similar) confidentiality restrictions as the THSA.
    c. Information received by the THSA is subject to public disclosure laws, such as Chapter 552, Texas Government Code ("Public Information Act"). If the THSA is required by operation of law to disclose Confidential Participant Information, including but not limited to the Public Information Act, the THSA will promptly notify the Participant or Applicant that provided the Confidential Participant Information. Such notification will include the terms and circumstances surrounding such operation of law. The information in the notification must be sufficient to allow the Participant or Applicant to exercise its rights to object to such disclosure. If, after the Participant's or Applicant's objection, the THSA is still required by law to disclose the Confidential Participant Information, the THSA shall do so only to the minimum extent necessary to comply with the operation of the law and shall request that the Confidential Participant Information be treated as such.

7. *Secure Disposal:* Hard copies and electronic versions of Confidential Participant Information shall be securely destroyed when such versions no longer require retention under Section 5. An audit log of any Confidential Participant Information shall be available for review by a Participant whose information was destroyed.

8. *Protected Health Information ("PHI"):* The THSA shall make every effort to perform its duties without requesting PHI or through the request, receipt and/or use of de-identified and/or aggregate data. If the THSA determines that PHI is needed for the full exercise of its duties under the State-Level Trust Agreement, it may request the needed PHI from the Applicant or Participant. The Applicant or Participant is not obligated to provide PHI to THSA in violation of Applicable Law. Should the THSA request and receive PHI, it shall be kept separate from all other information received and/or maintained by THSA and shall be subject to additional restrictions and/or agreements as determined by legal counsel and the submitting Applicant or Participant.

OPP 7: HIETexas Adverse Security Event Notification

I. Purpose

The privacy, security, and integrity of information exchanged are essential. To help maintain the privacy, security, and integrity of Information exchanged and promote trust among Participants, each Participant has agreed to notify certain other Participants and the THSA of an Adverse Security Event. This Policy sets forth the procedure by which a Participant and the THSA will fulfill their respective Adverse Security Event notification obligations under the State-Level Trust Agreement. For specific compliance with applicable state and federal medical privacy laws and regulations, such as HIPAA and Texas breach notification laws, please see the THSA's Privacy Policies and Procedures.

II. Policy

Adverse Security Events, as defined in the State-Level Trust Agreement, are very serious events with potential for serious impact on Participants and the individuals who's Protected Health Information (PHI) is transmitted in Messages via HIETexas. An adverse security event containing PHI shall be treated as "discovered" as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to the organization (i.e. adverse security events by the organization's business associates). Thus, each Participant has the obligation to identify, notify, investigate, and mitigate any known Adverse Security Event or potential Adverse Security Event, and when detection of a potential Adverse Security Event has occurred, the Participant will notify the THSA and any affected Participants of the potential Adverse Security Event in accordance with the procedures herein.

The THSA will conduct periodic reviews to evaluate and identify improvements to the Adverse Security Event Notification process.

III. Procedure

A. Adverse Security Event Notification Contact List

1. An authorized individual at the Participant's organization shall provide the THSA appropriate points of contact for Adverse Security Event Notification and shall promptly notify the THSA if those points of contact change by sending an email to ContactUpdateList@THSA.org. The Participant's organization is responsible for ensuring the THSA receives the notification described herein.
2. The THSA shall maintain an active list of Participant contacts for Adverse Security Event Notification purposes. The THSA shall make this list available to its Participants.
3. Participants are accountable for ensuring there are mechanisms within their respective organizations to notify appropriate individuals regarding Adverse Security Events.

B. One-Hour Adverse Security Event Alert

1. Within one (1) hour of discovering information that leads the Participant to reasonably believe that an Adverse Security Event **may have occurred or anticipate could reasonably occur**, the Participant will:

    a. Immediately notify the THSA of the potential Adverse Security Event by sending an email to BreachAlert@THSA.org (hereinafter "Alert Email"). This email is an inbound email account monitored by THSA staff; it is not an email distribution list that is suitable for notification to others outside the THSA.

        i. The Alert Email is primarily intended to alert that an Adverse Security Event may have occurred. Participants should use caution before relaying details of the potential Adverse Security Event via e-mail.

    b. Pursuant to Section 14.04 of the State-Level Trust Agreement, immediately notify other Participants, who, in the judgment of the Participant making the alert, may have had an Adverse Security Event of Information exchanged or otherwise are likely affected by the Adverse Security Event. Participants may rely upon the list of contacts described in Section (III)(A)(2) of this Policy in determining that proper notice under this Section has been sent to the correct contacts for all Participants likely affected by the Adverse Security Event.

2. Communication of Adverse Security Event Notification

    a. Adverse Security Event Notifications shall include the information described in Section 14.04 of the State-Level Trust Agreement.
    b. Participants are strongly urged to send Adverse Security Event Notifications through a secure means, where appropriate and possible (e.g. secure e-mail, posted on the Secure Site, etc.) and labeled as Confidential Participant Information.

3. If, on the basis of the information that the Participant has, the Participant believes that it should temporarily cease exchanging Information exchanged with all other Participants, it may undergo a service level interruption or voluntary suspension in accordance with Section 19.02 of the State-Level Trust Agreement.

C. Twenty-Four Hour Notification of Breach Determination

1. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining whether **an Adverse Security Event has occurred**, the Participant will:

    a. Immediately notify the THSA whether the Adverse Security Event occurred by sending notification through a secure means, where appropriate and possible (e.g. secure e-mail, posted on the Secure Site, etc.) and labeled as Confidential Participant Information.

    b. Send a notification of determination as to whether the Adverse Security Event occurred to other Participants who are likely impacted by the Adverse Security Event. Notifications sent to other Participants should be sent to the Adverse

Security Event Notification contact list. Participants may rely upon the list of contacts described in Section (III)(A)(2) of this Policy in determining that proper notice under this Section has been sent to the correct contacts for all Participants likely affected by the Adverse Security Event.

2. Participants are strongly urged to send Adverse Security Event Notifications through a secure means, where appropriate and possible (e.g. secure e-mail, posted on the Secure Site, etc.) and labeled as Confidential Participant Information. If the Adverse Security Event was determined to have occurred, the notification should include sufficient information for the THSA and other likely-impacted Participants to understand the nature of the Adverse Security Event. For instance, such notification could include, to the extent available at the time of the notification, the following information:

    - One or two sentence description of the Adverse Security Event
    - Description of the roles of the people involved in the Adverse Security Event (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)
    - The type of Information involved in the Adverse Security Event
    - Participants likely impacted by the Adverse Security Event
    - Number of individuals or records impacted/estimated to be impacted by the Adverse Security Event
    - Actions taken by the Participant to mitigate any unauthorized access to, use or disclosure of PHI as a result of the Adverse Security Event
    - Current Status of the Adverse Security Event (under investigation or resolved)
    - Corrective action taken and steps planned to be taken to prevent a similar Adverse Security Event.

The Notification shall not include any Protected Health Information (PHI). Participants are strongly urged to label the notification (e.g. subject line or posting, etc.) as Confidential Participant Information.

3. The Participant shall have a duty to supplement the information contained in the Notification as it becomes available. Supplemental information should be sent through a secure means (e.g. secure e-mail, posted on the Secure Site, etc.) and directed to the same addresses used for the original notification. Participants are strongly urged to label (e.g. subject line or posting, etc.) the supplemental information as Confidential Participant Information.
4. If, on the basis of the information that the Participant has, the Participant believes that it should temporarily cease exchanging Information exchanged with all other Participants, it may undergo a service level interruption or voluntary suspension in accordance with Section 19.02 of the State-Level Trust Agreement.

D. <u>THSA Disposition of Adverse Security Event Alerts and Notifications</u>

1. At the earliest possible time, the THSA shall schedule a remote or in-person meeting upon receipt of the Adverse Security Event alert and notification for the purpose of reviewing the notification and determining the following:

a. The impact of the Adverse Security Event or potential Adverse Security Event on the privacy, security and integrity of Information exchanged;

b. Whether the THSA needs to take any action to suspend the Participant(s) involved in the Adverse Security Event or potential Adverse Security Event in accordance with in accordance with Section 19.03 of the State-Level Trust Agreement;

c. Whether other Participants that have not been notified of the Adverse Security Event or potential Adverse Security Event would benefit from a summary of the notification or alert; or whether a summary of the notification or alert to the other Participants would enhance security; and,

   i. If the THSA determines that a summary should be distributed to Participants, the THSA will distribute such summary in a timely manner.

   ii. This summary shall not identify any of the Participants or individuals involved in the Adverse Security Event.

d. Whether the THSA should take any other measures in response to the notification or alert.

2. If a Participant reports a potential Adverse Security Event and later determines that an Adverse Security Event did not, in fact, occur, the THSA has final discretion regarding whether a meeting is necessary to discuss disposition of the event.

3. The THSA is permitted to request additional information from the Participant(s) involved in the Adverse Security Event or potential Adverse Security Event to fulfill its responsibilities. However, with respect to potential Adverse Security Event alerts, the THSA is encouraged to hold inquiries and requests for additional information to allow the Participant time to determine whether an Adverse Security Event actually occurred.

4. If, on the basis of the Adverse Security Event alert or notification, a Participant desires to cease exchanging Information exchanged with Participant(s) involved in the potential or actual Adverse Security Event, pursuant to the State-Level Trust Agreement, such Participant must notify the THSA of such cessation. The THSA shall maintain a log of all such cessations for the THSA's review.

5. If it is determined an Adverse Security Event occurred, once sufficient information about the Adverse Security Event becomes available, the THSA will, within a reasonable amount of time, determine whether the actions taken by the Participant(s) involved in the Adverse Security Event are adequate to mitigate the Adverse Security Event and prevent a similar Adverse Security Event from occurring in the future. Once the THSA is satisfied that the Participant(s) have taken all appropriate measures, the THSA will deem the Adverse Security Event resolved. Participants will update and inform the THSA as soon as possible regarding new information involving the Adverse Security Event.

   a. This resolution will be communicated to all Participant(s) involved in the Adverse Security Event and those Participants that ceased exchanging Information exchanged with the Participant(s) involved in the Adverse Security Event (if applicable).

   b. If a Participant does not resume the exchange of Information exchanged with the Participant(s) involved in the Adverse Security Event, such Participant(s) involved in the Adverse Security Event and cessation are encouraged to engage in the Dispute Resolution

Process pursuant to the State-Level Trust Agreement.

E. Adverse Security Event of PHI maintained by HIETexas.

If the THSA discovers, or through the exercise of reasonable diligence should have discovered, an Adverse Security Event, as defined in this this Policy and in the State-Level Trust Agreement, of PHI maintained by HIETexas, the THSA shall handle the notification and mitigation of such Adverse Security Event in accordance with the applicable Business Associate Agreement signed with each Participant, as well as Section 14.04 of the State-Level Trust Agreement.

IV. Definitions

Pursuant to Section 1(d) of the State Level Trust Agreement,

Adverse Security Event shall mean the unauthorized acquisition, access, disclosure, or use of unencrypted Message Content in the process of being transacted in a manner permitted by this Agreement by anyone who is not a Participant or Participant User of by a Participant or Participant User in any manner that is not a Permitted Purpose under this Agreement. For the avoidance of doubt, an "Adverse Security Event" under this Agreement does not include the following:

1. any unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of a Participant or Participant User if:

.01. such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participant or Participant User; and

.02. such unencrypted Message Content is not further acquired, accessed, disclosed or used by such employee or individual; or

2. any acquisition, access, disclosure or use of information contained in or available through the Participant's System where such acquisition, access, disclosure or use was not directly related to Transacting Message Content.

All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the State-Level Trust Agreement or the THSA Operating Policies and Procedures.

Attachment 2 – Applicable HIPAA provisions for Participants that are neither Covered Entities, Business Associates nor Governmental Participants

Pursuant to Section 14.01(d), the following HIPAA provisions are applicable to each Participant that is neither a Covered Entity, a Business Associate nor a Governmental Participant as if they were acting in the capacity of a Covered Entity. Definitions contained in the various provisions of 45 C.F.R. Parts 160 through 164 apply to the provisions listed in this Attachment 1 to the extent they are used in said sections.

- 45 C.F.R. § 164.306 (Security Rule – General rules)
- 45 C.F.R. § 164.308 (Security Rule – Administrative Safeguards)
- 45 C.F.R. § 164.310 (Security Rule – Physical Safeguards)
- 45 C.F.R. § 164.312 (Security Rule – Technical Safeguards)
- 45 C.F.R. § 164.314 (Security Rule – Organizational requirements)
- 45 C.F.R. § 164.316 (Security Rule – Policies and procedures and documentation requirements)
- 45 C.F.R. § 164.502, other than paragraphs (h), and (i) (Privacy Rule – Uses and disclosures of PHI: general rules) *[see notes below for descriptions of excluded subsections]*
- 45 C.F.R. § 164.504 (Privacy Rule – Uses and disclosures: Organizational requirements)
- 45 C.F.R. § 164.506 (Privacy Rule – Uses and disclosures to carry out treatment, payment, or health care operations)
- 45 C.F.R. § 164.508 (Privacy Rule – Uses and disclosures for which an authorization is required)
- 45 C.F.R. § 164.510 (Privacy Rule – Uses and disclosures requiring an opportunity to agree or to object)
- 45 C.F.R. § 164.512 (Privacy Rule – Uses and disclosures for which an authorization or opportunity to agree or object is not required)
- 45 C.F.R. § 164.514 (Privacy Rule – Other requirements relating to uses and disclosures of PHI)
- 45 C.F.R. § 164.520 (Privacy Rule – Notice of privacy practices for PHI)
- 45 C.F.R. § 164.522 (Privacy Rule – Rights to request privacy protection for PHI)
- 45 C.F.R. § 164.524 (Privacy Rule – Access of individuals to PHI)
- 45 C.F.R. § 164.528 (Privacy Rule – Accounting of disclosures of PHI)
- The following provisions of 45 C.F.R. § 160.530, but only to the extent that they relate to the above provisions. For example, with respect to 45 C.F.R. § 164.530(b), the Participant must provide training with respect to the above provisions, such as § 164.506, but not with respect to other provisions of the HIPAA Regulations, such as § 164.522.
    - 45 C.F.R. § 164.530(b) (Privacy Rule – Administrative Requirements, Training)
    - 45 C.F.R. § 164.530(c) (Privacy Rule – Administrative Requirements, Safeguards)

- o 45 C.F.R. § 164.530(d) (Privacy Rule – Administrative Requirements, Complaints to the Covered Entity)
- o 45 C.F.R. § 164.530(e) (Privacy Rule – Administrative Requirements, Sanctions) o 45 C.F.R. § 164.530(f) (Privacy Rule – Administrative Requirements, Mitigation) o 45 C.F.R. § 164.530(g) (Privacy Rule – Administrative Requirements, Refraining from intimidating or retaliatory acts)
- o 45 C.F.R. § 164.530(h) (Privacy Rule – Administrative Requirements, Waiver of rights)
- o 45 C.F.R. § 164.530(i) (Privacy Rule – Administrative Requirements, Policies and procedures)
- o 45 C.F.R. § 164.530(j) (Privacy Rule – Administrative Requirements, Documentation)

Notes:

The following requirements have not been included:

- 45 C.F.R. § 164.302 (Security Rule – Applicability)
- 45 C.F.R. § 164.304 (Security Rule – Definitions)
- 45 C.F.R. § 164.500 (Privacy Rule – Applicability)
- 45 C.F.R. § 164.501 (Privacy Rule – Definitions)
- 45 C.F.R. § 164.502(h) (Confidential communications), and (i) (Uses and disclosures consistent with notice)
- 45 C.F.R. § 164.526 (Privacy Rule – Amendment of PHI)
- 45 C.F.R. § 164.530(a) (Privacy Rule – Administrative Requirements, Personnel designations)
- 45 C.F.R. § 164.530(k) (Privacy Rule – Administrative Requirements, Group health plans)
- 45 C.F.R. § 164.532 (Privacy Rule – Transition provisions)

Attachment 3 - Dispute Resolution Process

When a Dispute arises, a Participant shall send written Notice, in accordance with the Notice provision in the Agreement, to the other Participant(s) involved in the Dispute. The notice must contain a summary of the issue as well as a recommendation for resolution. The Participant must send a copy of the notice to the THSA for informational purposes.

Within thirty (30) calendar days of receiving the notice, the Participants are obligated to meet and confer with each other, at least once in good faith and at a mutually agreeable location (or by telephone), to try to reach resolution (the "Informal Conference"). If the Participants reach a resolution at the Informal Conference, they shall provide Notification to that effect to the THSA.

If the Participants are unable to participate in an Informal Conference during the thirty (30) calendar day period or to reach resolution at the Informal Conference, they have ten (10) business days following the end of the thirty (30) calendar day period or the Informal Conference, respectively, in which to escalate the Dispute to the THSA in writing.

Once a Participant escalates a Dispute to the THSA, the THSA will have thirty (30) calendar days in which to convene a meeting of the involved Participants. During this meeting, each Participant shall be able to present its version of the Dispute and any information that it believes is pertinent to the THSA's decision.

a. The THSA shall have the ability to request additional information from the Participants to help it make its determination. The THSA, however, shall not have the authority to compel a response or the production of testimony or documents by the Participants.

b. The THSA is encouraged to develop an appropriate and equitable resolution of each submitted Dispute, considering all available evidence, the goals of the Agreement and other relevant considerations. The THSA must also have the authority to recommend sanctions for the breaching Participant. These sanctions include developing corrective action plans, suspension of participation rights, and termination of participation rights. The type of sanction will depend on the nature and severity of the breach.

c. Within fifteen (15) calendar days of the THSA Meeting, the THSA shall issue a written recommendation for resolution, including an explanation of the basis and rationale of its recommendation. If either Participant is dissatisfied with the THSA's recommendation for resolution, it shall have five (5) business days in which to appeal the Dispute to the THSA Board.

d. Within twenty (20) calendar days of receiving notice of escalation from a Participant, the THSA Board shall review the THSA's recommendation along with the information on which such recommendation was based and issue a final resolution. The THSA Board may seek additional information from the Participants to aid its resolution of the Dispute.

e. Within seven (7) calendar days of receiving the final resolution from the THSA Board, the Participants shall determine whether to accept or reject the resolution and so notify the THSA.

f. The THSA shall send a written summary of the resolution of the Dispute to all Participants. The summary will not identify the Participants involved, but will contain sufficient detail about the resolution to serve as an instructive resource for other Participants.

g. In no case shall a Participant be required to disclose PHI in violation of Applicable Law as part of its participation in the Dispute Resolution Process. The decision to not disclose PHI shall not be held against a Participant in the Dispute Resolution Process.

Attachment 4 – Joinder Agreement

This Joinder Agreement made as of the last date set forth below, by and between the THSA and _____ (the "New Participant") makes New Participant a party to that certain Health Information Exchange ("HIE") Texas ("HIETexas") State-Level Trust Agreement dated _____ among the Participants, as amended through the date hereof (the "Agreement").

RECITALS:

A. The New Participant desires to become a Participant and Transact Message Content with other Participants.

B. The THSA has accepted and approved the New Participant's application to become a Participant and Transact Message Content with other Participants, with the condition precedent that the New Participant executes this Joinder Agreement.

AGREEMENT:

NOW, THEREFORE, in consideration of good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the undersigned hereby agree as follows:

1. JOINDER. The New Participant is hereby made a party to the Agreement, and agrees to be bound by, and shall comply with, the terms thereof. From the date hereof, the New Participant shall be a Participant as that term is defined in the Agreement and shall be subject to all of the duties and obligations and entitled to the rights and benefits of a "Participant" as provided therein.

2. ACKNOWLEDGEMENT. The New Participant hereby acknowledges that it has received and reviewed a copy of the Agreement.

4. REAFFIRMATION. The terms and provisions of the Agreement remain in full force and effect in all respects.

5. COUNTERPARTS. This Joinder Agreement may be executed in any number of counterparts, each of which shall be an original, but all of which taken together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the undersigned have caused this Joinder Agreement to be executed, all as of the day and year first written above.

THSA	**NEW PARTICIPANT**
By: _____	By: _____
Name: _____	Name: _____
Date: _____	Date: _____

Attachment 5 - Business Associate Agreement

This Business Associate Addendum is made by and between _____ (INSERT NAME OF PARTICIPANT THAT WILL BE SHARING PHI AS PART OF THE USE CASE – REFERRED TO IN THIS TEMPLATE AS PARTICIPANT #1 FOR CLARITY) and _____ (INSERT NAME OF PARTICIPANT THAT WILL BE RECEIVING PHI AS PART OF THE USE CASE – REFERRED TO IN THIS TEMPLATE AS PARTICIPANT #2 FOR CLARITY). Each of PARTICIPANT #1 and PARTICIPANT #2 may be referred to herein as a "Party" or collectively as "Parties."

WHEREAS, PARTICIPANT #1 and PARTICIPANT #2 are each signatories to the HIETexas State-Level Trust Agreement which governs the Transaction of Message Content using HIETexas;

WHEREAS, PARTICIPANT #1, in its capacity as a Participant in HIETexas, will be providing Protected Health Information (PHI) as part of Transacting Message Content with PARTICIPANT #2 as part of its participation in HIETexas [INSERT NAME OF USE CASE] Use Case;

WHEREAS, the Parties have determined that they should have a business associate agreement among them to govern the use or disclosure of all PHI that is Transacted as part of the Use Case in which they are engaged.

NOW, THEREFORE, in consideration of the mutual promises contained in this Addendum, and other valuable consideration, the Parties agree as follows:

1. **Defined Terms**. Unless otherwise indicated below or elsewhere in this Addendum, all capitalized terms shall have the meanings provided in the HIETexas State-Level Trust Agreement or 45 C.F.R. 160.103, 164.103 and 164.501.

a. "Privacy Rule" means 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E, Standards for Privacy of Individually Identifiable Health Information.

b. "Protected Health Information" or "PHI" means individually identifiable health information as defined in 45 C.F.R. 160.103 that Participant receives or to which Participant has access.

c. "Security Rule" means 45 C.F.R. Part 164, Subpart C, Security Standards for the Protection of Electronic Protected Health Information.

2. **Modification of Agreement**. This Business Associate Addendum supplements the HIETexas State-Level Trust Agreement. The terms and provisions of this Business Associate Addendum shall control to the extent they are contrary, contradictory or inconsistent with the terms of the HIETexas State-Level Trust Agreement. Otherwise, the terms and provisions of the HIETexas State-Level Trust Agreement shall remain in full force and effect.

3. **Mutual Obligations**.

a. **Compliance with Privacy and Security Obligations**. Each Party agrees that the requirements of HIPAA and the HITECH Act that relate to the privacy and security of PHI, and are made applicable with respect to business associates, shall be applicable to them with respect to their participation in the Use Case.

b. **Limits on Use and Disclosure**. Except as otherwise limited in this Addendum, the Participant #2 may only use or disclose PHI to perform functions, activities, or services for, or on behalf of Participant #1 as specified in the Use Case and as permitted or required by applicable law and regulations. Except as otherwise limited in this Addendum, Participant #2 may also:

i. Use PHI for its proper management and administration or to carry out its legal responsibilities under the laws of the United States; and

ii. Disclose PHI for its proper management and administration, provided that disclosures are Required by Law, or Participant #2 obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and that the person will notify Participant #2 of any instances of which it was aware in which the confidentiality of the information may have been breached. The Participant #2 shall remain liable to Participant #1 for all acts or omissions of any third party to which it discloses PHI. Participant #1's written consent to such disclosure shall not relieve any other Participant #2 of such liability.

c. **Minimum Necessary**. Any use or disclosure of the PHI will be limited to the minimum PHI necessary for the permitted purpose and restricted to those employees, subcontractors or agents subject to a written obligation of confidentiality with Participant that is at least as protective of the PHI as this Addendum and permitted and/or required by Applicable Law. Participant #2 shall comply with any guidance issued by the Secretary regarding compliance with the minimum necessary standard.

d. **Safeguards**. Each Party will comply with all applicable provisions of Applicable Law including, but not limited to, the Privacy Rule and the Security Rule and will implement and maintain reasonable and appropriate administrative, physical and technical safeguards to protect the availability, integrity and confidentiality of the PHI as permitted and/or required by Applicable Law. Each Party shall also develop and implement policies and procedures and maintain documentation of such policies and procedures to assure compliance with Applicable Law including, but not limited to, the Privacy Rule and the Security Rule.

e. **Reports of Unauthorized Access, Use of Disclosure**. Participant #2 shall report in writing to Participant #1, without unreasonable delay, (i) any use or disclosure of PHI that is not authorized by this Addendum or the HIETexas State-Level Trust Agreement including, but not limited to, Adverse Security Events, defined in the HIETexas State-Level Trust Agreement, and (ii) any Breach of Unsecured Protected Health Information. Participant #2 shall deliver such notice not later than five (5) calendar days after the date on which Participant #2 (or any member of its workforce or its agent, except the person(s) responsible for the unauthorized use or disclosure or Breach, became aware, or in the exercise of reasonable diligence should have become aware, of such unauthorized use or disclosure or Breach. Notice of any unauthorized use or disclosure or Breach shall, if known, (i) describe the event resulting in the unauthorized use or disclosure or Breach; (ii) describe the types of PHI that were involved in the unauthorized disclosure or Breach; and (iii) describe what Participant #2 is doing to investigate, mitigate losses arising from and protect against any further unauthorized use or disclosure or Breach. Participant #2 shall maintain all documentation associated with the investigation of a potential unauthorized use or disclosure or Breach, including any information influencing its determination that the use or disclosure was or was not a Breach and any exceptions applied to the use or disclosure. On request, Participant #2 shall provide Participant #1 with the documentation relevant to the circumstances surrounding the unauthorized use or disclosure of Breach.

f. **Mitigation Procedures**. In the event of any improper use and/or disclosure of Protected Health Information, Participant #2 shall work cooperatively with Participant #1 to implement procedures for mitigating the harmful effects of such improper use and/or disclosure.

g. **Accounting of Disclosures**. In accordance with 45 C.F.R. Section 164.528, Participant #2 agrees to produce, and maintain for at least six (6) years, a record of any disclosure of the PHI, which record will include, for each disclosure, the date of disclosure, the name and address of the recipient, a description of the PHI disclosed (if known), the name of the individual who is the subject of the PHI (if known) and the

reason for disclosure. Upon request from Participant #1, Participant #2 will make its record of disclosure available to Participant #1 within the time frame and in the manner permitted and/or required by Applicable Law or as otherwise agreed by the Parties in writing. In the event the request for an accounting is delivered by an Individual directly to Participant #2, it shall forward such request to Participant #1.

h. **Access to Individuals**. Participant #2 agrees to provide Individuals with access to their Protected Health Information, as held in a Designated Record Set by Participant #2, in order to meet the requirements under 45 CFR Section 164.524, including in the electronic form or format requested by the Individual, as required by 45 CFR Section 164.524. In the event any individual requests access to Protected Health Information directly from Participant #2, it shall forward such request to Participant #1.

i. **Amendment of Protected Health Information**. Participant #2 agrees to make any amendment(s) to Protected Health Information it holds in a Designated Record Set, as requested by an Individual or directed by Participant #1 pursuant to 45 CFR Section 164.526. In the event the request for an amendment is delivered by an individual directly to Participant #2, it will promptly forward the request to Participant #1 and upon approval of Participant #1, amend the Protected Health Information and incorporate the amendment into its records.

j. **Right to Restrict**. Participant #2 agrees to comply with, upon communication from Participant #1, any restrictions to the use or disclosure of Protected Health Information that Participant #1 has agreed to in accordance with 45 CFR Section 164.522.

k. **Marketing/Sale of Protected Health Information**. Participant #2 shall not directly or indirectly receive remuneration in exchange for any Protected Health Information and shall not engage in marketing activities or the sale of Protected Health Information, as defined in the HIPAA Privacy & Security Rules or the Texas Medical Records Privacy Act, without the prior written consent of Participant #2 and individual written authorization, as required by law.

l. **De-Identification**. Upon the prior written approval of Participant #1, Participant #2 may use Protected Health Information to de-identify such information in accordance with 45 CFR Section 164.514.

m. **Aggregation**. Upon the prior written approval of Participant #1, Participant #2 may use Protected Health Information to provide Data Aggregation Services related to Participant #1's Health Care Operations, as permitted by 45 CFR Section 164.504€(2)(i)(B).

n. **Subcontractors**. Participant #2 shall ensure that any subcontractor to whom it provides PHI agrees to the same restrictions and conditions that apply through this Addendum and under Applicable Law to Participant #2. Participant #2 shall remain liable to Participant #1 for all acts or omissions of any subcontractor or agent to which Participant #2 discloses PHI; however, in no case shall Participant #2 be liable for any party who is under a direct contract with Participant #1. Participant #1's written consent to the use of subcontractors shall not relieve Participant #2 of liability under this section.

o. **Availability of Books and Records**. Participant #2 agrees to make its internal practices, books and records relating to its uses or disclosures of the PHI available to Participant #1, or, if directed in writing, the Secretary for purposes of determining compliance with Applicable Law, subject to attorney-client and other applicable priviliges.

p. **Participant #2's Performance of Participant #1's Obligations**. To the extent Participant #2 is to carry out one or more of Participant #1's or a Covered Entity's obligations under the Privacy Rule, at Subpart E of 45 C.F.R. Part 164, Participant #2 will comply with the requirements of the Privacy Rule that apply to Covered Entities in the performance of such obligations.

4. **Term and Termination**.

a. **Term**. This addendum shall become effective on the Effective Date of the implementation of the Use Case, unless the Parties otherwise mutually agree in writing to an alternative effective date.

b. **Termination**.

i. **Automatic Termination**. This Addendum will automatically terminate upon the termination or expiration of Participant #2's participation in the applicable Use Case or the termination of Participant #2's participation in HIETexas.

ii. **Material Breach of Business Associate Addendum**. Notwithstanding any provisions in this Addendum, any Party may terminate this Addendum if it determines that another Party has breached a material term of this Addendum and has not cured such breach within thirty (30) calendar days of receiving notice of the breach.

iii. **Effect of Termination**. Upon termination of the HIETexas State-Level Trust Agreement or this Addendum, Participant #2 will return or destroy the PHI, unless required otherwise by Applicable Law. If return or destruction of the PHI is not feasible, Participant #2 will extend the protections of this Addendum until

the PHI can be returned or destroyed. If Participant #2 elects to destroy the PHI, it will certify destruction upon Participant #1's written request.

5. **Independent Contractors**. In participating in the Use Case, Participant #2 will be acting as an independent contractor. Nothing contained in the HIETexas State-Level Trust Agreement or this Addendum shall be construed to create a partnership or a joint venture or to authorize Participant #2 to act as a general or special agent of Participant #1, except as specifically set forth in this Addendum or the HIETexas State-Level Trust Agreement.

6. Miscellaneous Terms. This addendum supersedes all prior understandings and agreements, written or oral, between the Parties with respect to its subject matter. This Addendum is incorporated into the HIETexas State-Level Trust Agreement. The section titles used in this Addendum are provided for convenience only and are not intended to affect the interpretation of any provision. Any ambiguity in this Addendum shall be resolved in favor of a meaning that permits the Parties to comply with Applicable Law. Any and all references in this Addendum to a statute or regulation mean the section as in effect or as amended. The Parties agree that if Applicable Law changes, this Addendum will be deemed to incorporate such changes as necessary for the Parties to operation in compliance with the amended or modified requirements of Applicable Law. Otherwise, this Addendum is to be construed as conferring any right, remedy or claim on any person or entity other than the Parties and their respective successors and assigns. This Addendum may not be assigned by any Party without express written consent of all other Parties. The unenforceability of any provision in this Addendum will not affect the enforceability of any other provision. The waiver of any right or obligation under this Addendum will not be deemed to be a continuing waiver or the waiver of another right or obligation. All waivers must be in writing and signed by both Parties. This Addendum may be executed in counterparts, which when considered together will constitute one and the same document. Facsimile or email transmission of a signed photocopy, facsimile document or other electronic image of this Addendum will be deemed delivery of an original.

The Parties hereby cause this Addendum to be signed by their duly authorized representative as of the date(s) below.

Participant #1

Organization: _____

Signature of Authorized Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Participant #2

Organization: _____

Signature of Authorized Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Attachment 6 – Validation Plan

The Validation Plan is available on the THSA's website at www.THSA.org/HIE/validation-plan/.