MEMORANDUM OF UNDERSTANDING
BETWEEN
DEPARTMENT OF STATE HEALTH SERVICES
AND
Collin County
DSHS CONTRACT NO. HHS001472800001

This Memorandum of Understanding (MOU) is between the Department of State Health Services (DSHS) and Collin County ("Local Public Health Entity" or "LHE"). DSHS and LHE may be referred to individually as a "Party" and collectively as the "Parties."

I. PURPOSE

DSHS agrees to provide LHE certain public health data and information, which DSHS maintains, for the purpose of providing essential public health services. This MOU provides the Parties' roles and responsibilities regarding access and utilization of the data as outlined in each attachment of this MOU.

II. LEGAL AUTHORITY

This MOU is entered into pursuant to Chapter 12 and 1001 of the Texas Health and Safety Code.

DSHS will provide public health data and information to LHE so that the LHE may provide "essential public health services" as defined in Section 121.002 of Texas Health and Safety Code, as follows:

- Monitor the health status of individuals in the community to identify community health problems;
- Diagnose and investigate community health problems and community health hazards;
- Inform, educate, and empower the community with respect to health issues;
- Mobilize community partnerships in identifying and solving community health problems;
- Develop policies and plans that support individual and community efforts to improve health;
- Enforce laws and rules that protect the public health and ensure safety in accordance with those laws and rules;
- Link individuals who have a need for community and personal health services to appropriate community and private providers;
- Ensure a competent workforce for the provision of essential public health services;
- Research new insights and innovative solutions to community health problems; and
- Evaluate the effectiveness, accessibility, and quality of personal and population-based health services in a community.

Legal authority for data and information sharing is authorized by and in compliance with 45 CFR Parts 160 and 164. Additional legal authority for data and information sharing for the data sets authorized to be shared under the MOU is specifically identified in a corresponding attachment to

this MOU.

DSHS will not share data or information until and unless data sets and elements are identified and incorporated into the MOU.

III. LHE JURISDICTION

The jurisdiction of the LHE under this MOU is Collin County.

To receive certain public health data and information for the contiguous jurisdiction(s), if permitted by the Section 1001.089 of the Texas Health and Safety Code, LHE shall submit written request to DSHS for review and approval. If DSHS authorizes the LHE to receive public health data and information for its contiguous jurisdiction(s), then DSHS Contract Representative will send written notice to the LHE specifying the approved contiguous jurisdiction(s) and the data type(s) that DSHS will make available to the LHE. After any testing, as determined appropriate by DSHS, LHE will receive written notice specifying when the public health data and information of the contiguous jurisdiction(s) will be made available.

IV. STATEMENT OF WORK

A. LHE shall:
   1. Comply with all DSHS policies and procedures regarding access and utilization of the data and information provided by DSHS.
   2. Access and receive the data and information in a secure, confidential manner in compliance with all applicable federal and state laws governing the protection of confidential information.
   3. Access, use and disclose the data and information for essential public health services only as set forth in this MOU.
   4. Promptly provide written notice to DSHS of any access, use or disclosure of the data and information which violates the terms of this MOU or applicable law.
   5. Submit a list of staff names, titles, and email addresses, and the intended uses of the data and information, to request and obtain access. The request must be submitted in writing to the DSHS Representatives identified in this MOU or through the agency's identity and access management system, based upon guidance provided by DSHS for each data set.
   6. Complete the data checklist(s) identified as attachments to this MOU, as applicable.
   7. Maintain a list of all authorized users with access to DSHS data and information, and upon written request by DSHS, provide the list of authorized users within five (5) business days.
   8. Notify the DSHS Representatives identified in this MOU or through the DSHS identity and access management system, based upon guidance provided by DSHS for each data set, of any changes in staff that require removal from the list of authorized users. Such notification must be made in writing or through the DSHS identity and access management system within five (5) business days of any staffing changes.
   9. On an annual basis, and as additionally requested by DSHS, certify the list of authorized users in writing to the DSHS Representatives identified in this MOU or through the DSHS identity and access management system, based upon guidance provided by DSHS for each data set.
   10. Submit an application for amendment to the DSHS Representatives identified in this

MOU to request changes or additional data set variables.

11. Participate in any required DSHS-sponsored training on the access and usage of the data and information.
12. Ensure the data and information provided to LHE under this MOU, including information residing on LHE's back-up systems, remains within the contiguous United States and such data and information shall not be accessed by individuals located outside of the contiguous United States. Furthermore, the data and information may not be received, stored, processed, or destroyed via information technology systems used by LHE that are located outside of the contiguous United States.

B. DSHS will:
1. Review the LHE's written requests for access to specific data and information and provide approval or denial of the request in writing or through the DSHS identity and access management system.
2. Conduct data user testing as determined appropriate by DSHS.
3. Notify the LHE when the data set(s) are available or authorized to be shared with the LHE.
4. After completion of testing protocols (such as user testing) and approval of LHE's submission of the information required under this MOU, make available certain public health data and information via a secure data exchange. Data and information sharing is limited to the data sets identified and submitted by the LHE and approved by DSHS under the MOU.
5. Deliver data and information through use of a secure file transfer protocol site or other method of data transfer with at least that same level of security and/or encryption.
6. Provide each approved LHE user with access credentials including the secure site, username, and password, as appropriate. This information will be provided directly to LHE staff members authorized to access the data and information.
7. Remove user access to the DSHS data and information as requested by LHE within five (5) business days of receipt of the LHE's written notification.
8. At its sole discretion, sponsor trainings and provide technical assistance on accessing the limited data sets through the DSHS databases.

C. The Parties will communicate as necessary to successfully manage this MOU and work in good faith together to fulfill the purpose of this MOU.

V. CONFIDENTIALITY

A. The Parties are required to comply with all applicable state and federal laws relating to the privacy, security, and confidentiality of the data and information.

B. LHE shall comply with the HHSC Data Use Agreement ("DUA") which is attached to this MOU as Attachment A.

C. LHE shall maintain appropriate procedural, administrative, physical, and technical safeguards to prevent the release or disclosure of any data and information obtained under this MOU to anyone other than individuals who are authorized by law to receive such records or information and who will protect the data and information from re-disclosure

as required by law. All data and information shall be maintained in a secure location and in compliance with the DUA.

D. LHE shall use the data and information obtained under this MOU only for purposes described in this MOU and in accordance with the terms under the MOU. In addition, LHE shall comply with LHE's appropriate review policies.

E. LHE shall not publish or disclose Confidential Data obtained or accessed under this MOU to a third party.

F. No Personally Identifiable Information ("PII") and non-public data may be accessed or disclosed by LHE without specific statutory authority and DSHS prior written approval.

G. Data and information no longer in use by LHE shall be destroyed using software that renders the data unrecoverable. LHE may not destroy data and information via information technology systems that are located outside the contiguous United States. Upon DSHS request, LHE shall provide written verification that the data and information has been destroyed.

H. LHE shall not attempt to link nor permit others to attempt to link the records of patients or individuals in the data sets with personally identifiable records from any other source.

I. LHE shall not release nor permit others to release any data or information that identifies individuals, directly or indirectly.

J. LHE shall not permit others to copy, sell, rent, license, lease, loan, or otherwise grant access to the data and information covered by this MOU to any other person or entity, unless approved in writing by DSHS.

K. LHE acknowledges that when releasing or disclosing the data set or any part to others in its organization it will retain full responsibility for the privacy and security of the data and information and will prohibit others from further release or disclosure of the data and information.

VI. DESIGNATION OF REPRESENTATIVES

The following will act as the representative authorized to administer activities under this MOU on behalf of its respective Party.

DSHS Contract Management Section (CMS)	DSHS Program	Collin County
Gretchen Wells, CTCM Contract Manager 1100 W 49th Street, MC 1990 Austin, Texas 78756 (512) 776-2679 Gretchen.Wells@dshs.texas.gov	Jason Lucas Branch Manager PO Box 149347 Mail Code 1898 Austin, TX 78714-9347 (512) 776-6439 HIRBrequests@dshs.texas.gov	Taylor Burton 825 N. McDonald #130 McKinney, Tx 75069 (972) 548-4464 tburton@co.collin.tx.us

Either Party may change its designated representative by providing written notice to the other Party.

VII. LEGAL NOTICES

Legal notices under this MOU shall be in writing and deemed delivered on the date of delivery if delivered by United States mail, postage paid, certified, return receipt requested; common carrier, overnight, signature required; or hand delivery. Legal Notices must be sent to the appropriate address below:

If to DSHS:
Health and Human Services Commission
Attention: Office of Chief Counsel
4601 W. Guadalupe, MC1100
Austin, Texas 78751

If to Local Health Entity
Collin County
Attn: Taylor Burton
825 N. McDonald #130
McKinney, Tx 75069

Copy To:
Department of State Health Services
Attn: General Counsel
1100 W. 49th Street, MC1919
Austin, Texas 78756

Copy To:
Collin County
Attn: Taylor Burton
825 N. McDonald #130
McKinney, Tx 75069

Notice may be given in an alternate manner with written approval from the other Party. Alternate notice shall be deemed effective upon written confirmation of receipt by the Party receiving notice.

Either Party may change its address for receiving legal notice by providing written notice to the other Party.

VIII. GENERAL TERMS AND CONDITIONS

A. Term of MOU

This MOU is effective on the date of the last Party to sign. This MOU will remain in effect

for two (2) years from the effective date, unless terminated sooner as provided herein.

B. Termination of the MOU

Termination without Cause. This MOU may be terminated by either Party by providing at least thirty (30) calendar days' advance written notice to the other Party.

Breach and Termination for Cause. DSHS may terminate this MOU immediately, and without prior notice, upon LHE's breach of the terms of this MOU. Such breach may include, but is not limited to, improper disclosure of the data and information or other violation of the privacy, confidentiality and/or security requirements set forth in this MOU.

Effect of Expiration or Termination. DSHS will cease data and information sharing immediately upon the expiration or termination of this MOU. Upon termination or expiration, LHE shall destroy all data and information using software that renders the data and information unrecoverable and provide documentation to DSHS that data and information was destroyed as directed by DSHS. LHE may not destroy data and information via information technology systems that are located outside the contiguous United States.

C. No Cost

This is a no cost agreement. Each Party shall pay the cost of its participation in this MOU without cost or reimbursement by the other Party.

D. DSHS Suspension of Information Sharing under this MOU

DSHS may temporarily suspend the sharing of data and information without advance notice and may restore access at a time, and in a manner, of its sole discretion.

E. Amendment

This MOU may be amended or modified by the consent of both Parties at any time during its term. Amendments to this MOU must be in writing and signed by authorized representatives of DSHS and LHE. No change in, addition to, or waiver of any term or condition of this MOU shall be binding on DSHS unless approved in writing by an authorized representative of DSHS.

F. Change in Laws and Compliance with Laws

The Parties shall comply with all applicable federal and state statutes, rules, and regulations. Any alterations, additions, or deletions to the terms of this MOU which are required by changes in federal or state law or regulations are automatically incorporated into the MOU without written amendment hereto and shall become effective on the date designated by such law or by regulation.

G. Permitting and Licensure

LHE shall obtain and maintain for the duration of this MOU any state, county, city, or federal license, authorization, insurance, waiver, permit, qualification, or certification required by

statute, ordinance, law, or regulation to assume the roles and responsibilities contained within this MOU.

H. Assignment

LHE shall not assign its rights under this MOU or delegate the performance of its duties under the MOU without prior written approval from DSHS. Any attempted assignment in violation of this provision is void and without effect.

I. No Partnership or Joint Venture

The Parties agree that nothing in this MOU shall be deemed to create an association, partnership, or joint venture between DSHS and LHE.

J. No Waiver

Failure of either Party to insist on strict compliance with any term or condition of this MOU or to exercise any right or privilege hereunder will not be deemed a waiver of such term, condition, right or privilege later.

K. Severability

If any provision of this MOU is illegal, invalid, void, or unenforceable, the other provisions of this MOU will not be affected. The Parties agree to amend any illegal, invalid, void, or unenforceable provision to the extent necessary to render it valid, legal, and enforceable while preserving the intent of the MOU.

L. Disaster Recovery Plan

Upon request of DSHS, LHE shall provide copies of its most recent business continuity and disaster recovery plans.

M. Dispute Resolution

The Parties agree to use good faith efforts to resolve all questions, difficulties, or disputes of any nature that may arise under or by this MOU. However, nothing in this paragraph shall preclude either Party from pursuing any remedies as may be available under Texas law. Notwithstanding this provision, the Parties acknowledge and agree to use the dispute resolution provisions required under Chapter 2260 of the Texas Government Code, to the extent applicable.

N. Indemnification

LHE SHALL DEFEND, INDEMNIFY AND HOLD HARMLESS THE STATE OF TEXAS AND DSHS, AND/OR THEIR OFFICERS, AGENTS, EMPLOYEES, REPRESENTATIVES, CONTRACTORS, ASSIGNEES, AND/OR DESIGNEES FROM ANY AND ALL LIABILITY, ACTIONS, CLAIMS, DEMANDS, OR SUITS, AND ALL RELATED COSTS, ATTORNEY FEES, AND EXPENSES ARISING OUT OF OR RESULTING FROM ANY ACTS OR OMISSIONS OF LHE OR ITS AGENTS,

EMPLOYEES, SUBCONTRACTORS, ORDER FULFILLERS, OR SUPPLIERS OF SUBCONTRACTORS IN THE EXECUTION OR PERFORMANCE OF THE MOU. THIS CLAUSE IS NOT INTENDED TO AND WILL NOT BE CONSTRUED TO REQUIRE LHE TO INDEMNIFY OR HOLD HARMLESS THE STATE OR DSHS FOR ANY CLAIMS OR LIABILITIES RESULTING FROM THE NEGLIGENT ACTS OR OMISSIONS OF DSHS OR ITS EMPLOYEES. FOR THE AVOIDANCE OF DOUBT, DSHS SHALL NOT INDEMNIFY LHE OR ANY OTHER ENTITY UNDER THE MOU.

O. Force Majeure

Neither Party shall be liable to the other for any delay in, or failure of performance of, any requirement included in this MOU caused by force majeure. The existence of such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been removed provided the non-performing Party exercises all reasonable due diligence to perform. Force majeure is defined as acts of God, war, fires, explosions, hurricanes, floods, failure of transportation, or other causes that are beyond the reasonable control of either Party and that by exercise of due foresight such Party could not reasonably have been expected to avoid, and which, by the exercise of all reasonable due diligence, such Party is unable to overcome.

P. Public Information Act

Each Party is responsible for complying with Chapter 552 of the Texas Government Code ("Texas Public Information Act") as interpreted by judicial decisions and opinions of the Attorney General of Texas. Responses to requests for information and open records requests shall be handled in accordance with the provisions of the Texas Public Information Act.

Q. Limitation on Authority

LHE shall have no authority to act for or on behalf of DSHS or the State of Texas except as expressly provided for in this MOU; no other authority, power or use is granted or implied. LHE may not incur any debt, obligation, expense or liability of any kind on behalf of DSHS or the State of Texas.

R. Survival

Expiration or termination of this MOU for any reason does not release LHE from any liability or obligation set forth in this MOU that is expressly stated to survive any such expiration or termination, or that by its nature would be intended to be applicable following any such expiration or termination, or that is necessary to fulfill the essential purpose of the MOU, including without limitation the provisions regarding confidentiality and rights and remedies upon termination.

S. Sovereign Immunity

This MOU shall not constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies, or immunities available to either Party as an agency of the State of Texas or otherwise available to the Party. The failure to enforce or any delay in the enforcement of

any privileges, rights, defenses, remedies, or immunities available to a Party under this MOU or under applicable law shall not constitute a waiver of such privileges, rights, defenses, remedies, or immunities or be considered as a basis for estoppel. Neither Party waives any privileges, rights, defenses, or immunities available to it as an agency of the State of Texas, or otherwise available to it, by entering into this MOU or by its conduct prior to or subsequent to entering into this MOU.

T. Agency's Right to Audit

LHE shall make available at reasonable times and upon reasonable notice, and for reasonable periods, work papers, reports, books, records, and supporting documents kept current by LHE pertaining to the MOU for purposes of inspecting, monitoring, auditing, or evaluating by DSHS and the State of Texas.

U. State Auditor's Right to Audit

The state auditor may conduct an audit or investigation of any entity receiving funds from the state directly under the MOU or indirectly through a subcontract under the MOU. The acceptance of funds directly under the MOU or indirectly through a subcontract under the contract acts as acceptance of the authority of the state auditor, under the direction of the legislative audit committee, to conduct an audit or investigation in connection with those funds. Under the direction of the legislative audit committee, an entity that is the subject of an audit or investigation by the state auditor must provide the state auditor with access to any information the state auditor considers relevant to the investigation or audit.

V. MOU Attachments

The following documents are attached hereto, incorporated herein, and made a part of this MOU for all purposes:

1. Attachment A: HHS Data Use Agreement—TACCHO Version
2. Attachment B: Access to Public Health Dashboards
3. Attachment C: Access to Vital Event Data
4. Attachment D: Access to Texas Health Care Information Collection Public Use Data File

In the event of conflict, ambiguity, or inconsistency between or among any documents, all DSHS documents take precedence over LHE documents, and the HHS Data Use Agreement takes precedence over all other MOU documents.

W. Governing Law and Venue

This MOU shall be governed by and construed in accordance with the laws of the State of Texas, without regard to the conflicts of law provisions. The venue of any suit arising under the MOU is fixed in any court of competent jurisdiction of Travis County, Texas.

X. Counterparts and Signatures

The Parties may sign this MOU in counterparts, each of which will be deemed an original,

but all of which will together constitute one document. Electronically transmitted signatures will be deemed originals for all purposes related to this MOU.

Y. Entire Agreement

This document constitutes the entire agreement of the Parties and is intended as a complete and exclusive statement of the promises, representations, negotiations, discussions, and other agreements that may have been made in connection with the subject matter hereof. Any additional or conflicting terms in any future document incorporated into this agreement will be harmonized with this agreement to the extent possible.

Z. Signature Authority

By signing below, the Parties agree that they have read the MOU and agree to its terms, and that the persons whose signatures appear below have the authority to execute this MOU on behalf of their respective Party.

SIGNATURE PAGE FOLLOWS

SIGNATURE PAGE
DSHS Contract No. HHS001472800001

Department of State Health Services	**Collin County**
Signature of Authorized Official	Signature of Authorized Official
Printed Name	Printed Name
Title	Title
Date	Date

ATTACHMENT A

HHS DATA USE AGREEMENT

This Data Use Agreement ("DUA"), effective as of the date the Base Contract into which it is incorporated is signed ("Effective Date"), is entered into by and between a Texas Health and Human Services Enterprise agency ("HHS"), and the Contractor identified in the Base Contract, a political subdivision of the State of Texas ("CONTRACTOR.

ARTICLE 1.
PURPOSE; APPLICABILITY; ORDER OF PRECEDENCE

The purpose of this DUA is to facilitate creation, receipt, maintenance, use, disclosure or access to Confidential Information with CONTRACTOR, and describe CONTRACTOR's rights and obligations with respect to the Confidential Information. ***45 CFR 164.504(e)(1)-(3)***. This DUA also describes HHS's remedies in the event of CONTRACTOR's noncompliance with its obligations under this DUA. This DUA applies to both Business Associates and contractors who are not Business Associates who create, receive, maintain, use, disclose or have access to Confidential Information on behalf of HHS, its programs or clients as described in the Base Contract.

As of the Effective Date of this DUA, if any provision of the Base Contract, including any General Provisions or Uniform Terms and Conditions, conflicts with this DUA, this DUA controls.

ARTICLE 2.
DEFINITIONS

For the purposes of this DUA, capitalized, underlined terms have the meanings set forth in the following: Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (42 U.S.C. §1320d, *et seq.*) and regulations thereunder in 45 CFR Parts 160 and 164, including all amendments, regulations and guidance issued thereafter; The Social Security Act, including Section 1137 (42 U.S.C. §§ 1320b-7), Title XVI of the Act; The Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a and regulations and guidance thereunder; Internal Revenue Code, Title 26 of the United States Code and regulations and publications adopted under that code, including IRS Publication 1075; OMB Memorandum 07-18; Texas Business and Commerce Code Ch. 521; Texas Government Code, Ch. 552, and Texas Government Code §2054.1125. In addition, the following terms in this DUA are defined as follows:

"Authorized Purpose" means the specific purpose or purposes described in the Statement of Work of the Base Contract for CONTRACTOR to fulfill its obligations under the Base Contract, or any other purpose expressly authorized by HHS in writing in advance.

"Authorized User" means a Person:

(1) Who is authorized to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze Confidential Information pursuant to this DUA;

(2) For whom CONTRACTOR warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to the Confidential Information; and

(3) Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information as required by this DUA.

"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to CONTRACTOR, or that CONTRACTOR may, for an Authorized Purpose, create, receive, maintain, use, disclose or have access to, that consists of or includes any or all of the following:

(1) Client Information;

(2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information (herein "PHI");

(3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;

(4) Federal Tax Information;

(5) Individually Identifiable Health Information as related to HIPAA, Texas HIPAA and Personal Identifying Information under the Texas Identity Theft Enforcement and Protection Act;

(6) Social Security Administration Data, including, without limitation, Medicaid information;

(7) All privileged work product;

(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

"Legally Authorized Representative" of the Individual, as defined by Texas law, including as provided in 45 CFR 435.923 (Medicaid); 45 CFR 164.502(g)(1) (HIPAA); Tex. Occ. Code § 151.002(6); Tex. H. & S. Code §166.164; and Estates Code Ch. 752.

ARTICLE 3.
CONTRACTOR'S DUTIES REGARDING CONFIDENTIAL INFORMATION

3.01 Obligations of CONTRACTOR

CONTRACTOR agrees that:

(A) CONTRACTOR will exercise reasonable care and no less than the same degree of care CONTRACTOR uses to protect its own confidential, proprietary and trade secret information to prevent any portion of the Confidential Information from being used in

a manner that is not expressly an Authorized Purpose under this DUA or as Required by Law. ***45 CFR 164.502(b)(1); 45 CFR 164.514(d)***

(B) Except as Required by Law, CONTRACTOR will not disclose or allow access to any portion of the Confidential Information to any Person or other entity, other than Authorized User's Workforce or Subcontractors (as defined in ***45 C.F.R. 160.103***) of CONTRACTOR who have completed training in confidentiality, privacy, security and the importance of promptly reporting any Event or Breach to CONTRACTOR's management, to carry out CONTRACTOR's obligations in connection with the Authorized Purpose.

HHS, at its election, may assist CONTRACTOR in training and education on specific or unique HHS processes, systems and/or requirements. CONTRACTOR will produce evidence of completed training to HHS upon request. ***45 C.F.R. 164.308(a)(5)(i); Texas Health & Safety Code §181.101***

All of CONTRACTOR's Authorized Users, Workforce and Subcontractors with access to a state computer system or database will complete a cybersecurity training program certified under Texas Government Code Section 2054.519 by the Texas Department of Information Resources.

(C) CONTRACTOR will establish, implement and maintain appropriate sanctions against any member of its Workforce or Subcontractor who fails to comply with this DUA, the Base Contract or applicable law. CONTRACTOR will maintain evidence of sanctions and produce it to HHS upon request.***45 C.F.R. 164.308(a)(1)(ii)(C); 164.530(e); 164.410(b); 164.530(b)(1)***

(D) CONTRACTOR will not, except as otherwise permitted by this DUA, disclose or provide access to any Confidential Information on the basis that such act is Required by Law without notifying either HHS or CONTRACTOR's own legal counsel to determine whether CONTRACTOR should object to the disclosure or access and seek appropriate relief. CONTRACTOR will maintain an accounting of all such requests for disclosure and responses and provide such accounting to HHS within 48 hours of HHS' request. ***45 CFR 164.504(e)(2)(ii)(A)***

(E) CONTRACTOR will not attempt to re-identify or further identify Confidential Information or De-identified Information, or attempt to contact any Individuals whose records are contained in the Confidential Information, except for an Authorized Purpose, without express written authorization from HHS or as expressly permitted by the Base Contract. ***45 CFR 164.502(d)(2)(i) and (ii)*** CONTRACTOR will not engage in prohibited marketing or sale of Confidential Information. ***45 CFR 164.501, 164.508(a)(3) and (4); Texas Health & Safety Code Ch. 181.002***

(F) CONTRACTOR will not permit, or enter into any agreement with a Subcontractor to, create, receive, maintain, use, disclose, have access to or transmit Confidential Information to carry out CONTRACTOR's obligations in connection with the Authorized Purpose on behalf of CONTRACTOR, unless Subcontractor agrees to comply with all applicable laws, rules and regulations. ***45 CFR 164.502(e)(1)(ii); 164.504(e)(1)(i) and (2).***

(G) CONTRACTOR is directly responsible for compliance with, and enforcement of, all conditions for creation, maintenance, use, disclosure, transmission and Destruction of Confidential Information and the acts or omissions of Subcontractors as may be reasonably necessary to prevent unauthorized use. ***45 CFR 164.504(e)(5); 42 CFR 431.300, et seq.***

(H) If CONTRACTOR maintains PHI in a Designated Record Set which is Confidential Information and subject to this Agreement, CONTRACTOR will make PHI available to HHS in a Designated Record Set upon request. CONTRACTOR will provide PHI to an Individual, or Legally Authorized Representative of the Individual who is requesting PHI in compliance with the requirements of the HIPAA Privacy Regulations. CONTRACTOR will release PHI in accordance with the HIPAA Privacy Regulations upon receipt of a valid written authorization. CONTRACTOR will make other Confidential Information in CONTRACTOR's possession available pursuant to the requirements of HIPAA or other applicable law upon a determination of a Breach of Unsecured PHI as defined in HIPAA. CONTRACTOR will maintain an accounting of all such disclosures and provide it to HHS within 48 hours of HHS' request. ***45 CFR 164.524and 164.504(e)(2)(ii)(E).***

(I) If PHI is subject to this Agreement, CONTRACTOR will make PHI as required by HIPAA available to HHS for review subsequent to CONTRACTOR's incorporation of any amendments requested pursuant to HIPAA. ***45 CFR 164.504(e)(2)(ii)(E) and (F).***

(J) If PHI is subject to this Agreement, CONTRACTOR will document and make available to HHS the PHI required to provide access, an accounting of disclosures or amendment in compliance with the requirements of the HIPAA Privacy Regulations. ***45 CFR 164.504(e)(2)(ii)(G) and 164.528.***

(K) If CONTRACTOR receives a request for access, amendment or accounting of PHI from an individual with a right of access to information subject to this DUA, it will respond to such request in compliance with the HIPAA Privacy Regulations. CONTRACTOR will maintain an accounting of all responses to requests for access to or amendment of PHI and provide it to HHS within 48 hours of HHS' request. ***45 CFR 164.504(e)(2).***

(L) CONTRACTOR will provide, and will cause its Subcontractors and agents to provide, to HHS periodic written certifications of compliance with controls and provisions relating to information privacy, security and breach notification, including without limitation information related to data transfers and the handling and disposal of Confidential Information. ***45 CFR 164.308; 164.530(c); 1 TAC 202.***

(M) Except as otherwise limited by this DUA, the Base Contract, or law applicable to the Confidential Information, CONTRACTOR may use PHI for the proper management and administration of CONTRACTOR or to carry out CONTRACTOR's legal responsibilities. Except as otherwise limited by this DUA, the Base Contract, or law applicable to the Confidential Information, CONTRACTOR may disclose PHI for the

proper management and administration of CONTRACTOR, or to carry out CONTRACTOR's legal responsibilities, if: ***45 CFR 164.504(e)(4)(A).***

(1) Disclosure is Required by Law, provided that CONTRACTOR complies with Section 3.01(D); or

(2) CONTRACTOR obtains reasonable assurances from the person or entity to which the information is disclosed that the person or entity will:

(a)Maintain the confidentiality of the Confidential Information in accordance with this DUA;

(b) Use or further disclose the information only as Required by Law or for the Authorized Purpose for which it was disclosed to the Person; and

(c)Notify CONTRACTOR in accordance with Section 4.01 of any Event or Breach of Confidential Information of which the Person discovers or should have discovered with the exercise of reasonable diligence. ***45 CFR 164.504(e)(4)(ii)(B).***

(N) Except as otherwise limited by this DUA, CONTRACTOR will, if required by law and requested by HHS, use commercially reasonable efforts to use PHI to provide data aggregation services to HHS, as that term is defined in the HIPAA, 45 C.F.R. §164.501 and permitted by HIPAA. ***45 CFR 164.504(e)(2)(i)(B)***

(O) CONTRACTOR will, on the termination or expiration of this DUA or the Base Contract, at its expense, send to HHS or Destroy, at HHS's election and to the extent reasonably feasible and permissible by law, all Confidential Information received from HHS or created or maintained by CONTRACTOR or any of CONTRACTOR's agents or Subcontractors on HHS's behalf if that data contains Confidential Information. CONTRACTOR will certify in writing to HHS that all the Confidential Information that has been created, received, maintained, used by or disclosed to CONTRACTOR, has been Destroyed or sent to HHS, and that CONTRACTOR and its agents and Subcontractors have retained no copies thereof. Notwithstanding the foregoing, HHS acknowledges and agrees that CONTRACTOR is not obligated to send to HHSC and/or Destroy any Confidential Information if federal law, state law, the Texas State Library and Archives Commission records retention schedule, and/or a litigation hold notice prohibit such delivery or Destruction. If such delivery or Destruction is not reasonably feasible, or is impermissible by law, CONTRACTOR will immediately notify HHS of the reasons such delivery or Destruction is not feasible, and agree to extend indefinitely the protections of this DUA to the Confidential Information and limit its further uses and disclosures to the purposes that make the return delivery or Destruction of the Confidential Information not feasible for as long as CONTRACTOR maintains such Confidential Information. ***45 CFR 164.504(e)(2)(ii)(J)***

(P) CONTRACTOR will create, maintain, use, disclose, transmit or Destroy Confidential Information in a secure fashion that protects against any reasonably anticipated

threats or hazards to the security or integrity of such information or unauthorized uses. ***45 CFR 164.306; 164.530(c)***

(Q) If CONTRACTOR accesses, transmits, stores, and/or maintains Confidential Information, CONTRACTOR will complete and return to HHS at infosecurity@hhsc.state.tx.us the HHS information security and privacy initial inquiry (SPI) at Attachment 1 . The SPI identifies basic privacy and security controls with which CONTRACTOR must comply to protect HHS Confidential Information. CONTRACTOR will comply with periodic security controls compliance assessment and monitoring by HHS as required by state and federal law, based on the type of Confidential Information CONTRACTOR creates, receives, maintains, uses, discloses or has access to and the Authorized Purpose and level of risk. CONTRACTOR's security controls will be based on the National Institute of Standards and Technology (NIST) Special Publication 800-53. CONTRACTOR will update its security controls assessment whenever there are significant changes in security controls for HHS Confidential Information and will provide the updated document to HHS. HHS also reserves the right to request updates as needed to satisfy state and federal monitoring requirements. ***45 CFR 164.306.***

(R) CONTRACTOR will establish, implement and maintain reasonable procedural, administrative, physical and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of the Confidential Information, and with respect to PHI, as described in the HIPAA Privacy and Security Regulations, or other applicable laws or regulations relating to Confidential Information, to prevent any unauthorized use or disclosure of Confidential Information as long as CONTRACTOR has such Confidential Information in its actual or constructive possession. ***45 CFR 164.308 (administrative safeguards); 164.310 (physical safeguards); 164.312 (technical safeguards); 164.530(c)(privacy safeguards).***

(S) CONTRACTOR will designate and identify, a Person or Persons, as Privacy Official ***45 CFR 164.530(a)(1)*** and Information Security Official, each of whom is authorized to act on behalf of CONTRACTOR and is responsible for the development and implementation of the privacy and security requirements in this DUA. CONTRACTOR will provide name and current address, phone number and e-mail address for such designated officials to HHS upon execution of this DUA and prior to any change. If such persons fail to develop and implement the requirements of the DUA, CONTRACTOR will replace them upon HHS request. ***45 CFR 164.308(a)(2).***

(T) CONTRACTOR represents and warrants that its Authorized Users each have a demonstrated need to know and have access to Confidential Information solely to the minimum extent necessary to accomplish the Authorized Purpose pursuant to this DUA and the Base Contract, and further, that each has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information contained in this DUA. ***45 CFR 164.502; 164.514(d).***

(U) CONTRACTOR and its Subcontractors will maintain an updated, complete, accurate and numbered list of Authorized Users, their signatures, titles and the date they

agreed to be bound by the terms of this DUA, at all times and supply it to HHS, as directed, upon request.

(V) CONTRACTOR will implement, update as necessary, and document reasonable and appropriate policies and procedures for privacy, security and Breach of Confidential Information and an incident response plan for an Event or Breach, to comply with the privacy, security and breach notice requirements of this DUA prior to conducting work under the Statement of Work. ***45 CFR 164.308; 164.316; 164.514(d); 164.530(i)(1).***

(W) CONTRACTOR will produce copies of its information security and privacy policies and procedures and records relating to the use or disclosure of Confidential Information received from, created by, or received, used or disclosed by CONTRACTOR for an Authorized Purpose for HHS's review and approval within 30 days of execution of this DUA and upon request by HHS the following business day or other agreed upon time frame. ***45 CFR 164.308; 164.514(d).***

(X) CONTRACTOR will make available to HHS any information HHS requires to fulfill HHS's obligations to provide access to, or copies of, PHI in accordance with HIPAA and other applicable laws and regulations relating to Confidential Information. CONTRACTOR will provide such information in a time and manner reasonably agreed upon or as designated by the Secretary of the U.S. Department of Health and Human Services, or other federal or state law. ***45 CFR 164.504(e)(2)(i)(I).***

(Y) CONTRACTOR will only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form, in accordance with applicable rules, regulations and laws. A secure transmission of electronic Confidential Information *in motion* includes, but is not limited to, Secure File Transfer Protocol (SFTP) or Encryption at an appropriate level. If required by rule, regulation or law, HHS Confidential Information *at rest* requires Encryption unless there is other adequate administrative, technical, and physical security. All electronic data transfer and communications of Confidential Information will be through secure systems. Proof of system, media or device security and/or Encryption must be produced to HHS no later than 48 hours after HHS's written request in response to a compliance investigation, audit or the Discovery of an Event or Breach. Otherwise, requested production of such proof will be made as agreed upon by the parties. De-identification of HHS Confidential Information is a means of security. With respect to de-identification of PHI, "secure" means de-identified according to HIPAA Privacy standards and regulatory guidance. ***45 CFR 164.312; 164.530(d).***

(Z) For each type of Confidential Information CONTRACTOR creates, receives, maintains, uses, discloses, has access to or transmits in the performance of the Statement of Work, CONTRACTOR will comply with the following laws rules and regulations, only to the extent applicable and required by law:

- Title 1, Part 10, Chapter 202, Subchapter B, Texas Administrative Code;
- The Privacy Act of 1974;

- OMB Memorandum 07-16;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) as defined in the DUA;
- Internal Revenue Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies;
- National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- NIST Special Publications 800-53 and 800-53A – Recommended Security Controls for Federal Information Systems and Organizations, as currently revised;
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems;
- NIST Special Publication 800-88, Guidelines for Media Sanitization;
- NIST Special Publication 800-111, Guide to Storage of Encryption Technologies for End User Devices containing PHI; and

Any other State or Federal law, regulation, or administrative rule relating to the specific HHS program area that CONTRACTOR supports on behalf of HHS.

(AA) Notwithstanding anything to the contrary herein, CONTRACTOR will treat any Personal Identifying Information it creates, receives, maintains, uses, transmits, destroys and/or discloses in accordance with Texas Business and Commerce Code, Chapter 521 and other applicable regulatory standards identified in Section 3.01(Z), and Individually Identifiable Health Information CONTRACTOR creates, receives, maintains, uses, transmits, destroys and/or discloses in accordance with HIPAA and other applicable regulatory standards identified in Section 3.01(Z).

ARTICLE 4.
BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS

4.01 Breach or Event Notification to HHS. 45 CFR 164.400-414.

(A) CONTRACTOR will cooperate fully with HHS in investigating, mitigating to the extent practicable and issuing notifications directed by HHS, for any Event or Breach of Confidential Information to the extent and in the manner determined by HHS.

(B) CONTRACTOR'S obligation begins at the Discovery of an Event or Breach and continues as long as related activity continues, until all effects of the Event are mitigated to HHS's reasonable satisfaction (the "incident response period"). ***45 CFR 164.404.***

(C) Breach Notice:

(1) Initial Notice.

(a) For federal information, including without limitation, Federal Tax Information, Social Security Administration Data, and Medicaid Client Information, within the first, consecutive clock hour of Discovery, and for all other types of Confidential Information not more than 24 hours after Discovery, or in a timeframe otherwise approved by HHS in writing, initially report to HHS's Privacy and Security Officers via email at: privacy@HHSC.state.tx.us and to the HHS division responsible for this DUA; and IRS Publication 1075; Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a; OMB Memorandum 07-16 as cited in HHSC-CMS Contracts for information exchange.

(b) Report all information reasonably available to CONTRACTOR about the Event or Breach of the privacy or security of Confidential Information. ***45 CFR 164.410.***

(c) Name, and provide contact information to HHS for, CONTRACTOR's single point of contact who will communicate with HHS both on and off business hours during the incident response period.

(2) Formal Notice. No later than two business days after the Initial Notice above, provide formal notification to privacy@HHSC.state.tx.us and to the HHS division responsible for this DUA, including all reasonably available information about the Event or Breach, and CONTRACTOR's investigation, including without limitation and to the extent available***: For (a) - (m) below: 45 CFR 164.400-414.***

(a) The date the Event or Breach occurred;

(b) The date of CONTRACTOR's and, if applicable, Subcontractor's Discovery;

(c) A brief description of the Event or Breach; including how it occurred and who is responsible (or hypotheses, if not yet determined);

(d) A brief description of CONTRACTOR's investigation and the status of the investigation;

(e) A description of the types and amount of Confidential Information involved;

(f) Identification of and number of all Individuals reasonably believed to be affected, including first and last name of the Individual and if applicable the, Legally Authorized Representative, last known address, age, telephone number, and email address if it is a preferred contact method, to the extent known or can be reasonably determined by CONTRACTOR at that time;

(g) CONTRACTOR's initial risk assessment of the Event or Breach demonstrating whether individual or other notices are required by applicable law or this DUA for HHS approval, including an analysis of whether there is a low probability of compromise of the Confidential Information or whether any legal exceptions to notification apply;

(h) CONTRACTOR's recommendation for HHS's approval as to the steps Individuals and/or CONTRACTOR on behalf of Individuals, should take to protect the Individuals from potential harm, including without limitation CONTRACTOR's provision of notifications, credit protection, claims monitoring, and any specific protections for a Legally Authorized Representative to take on behalf of an Individual with special capacity or circumstances;

(i) The steps CONTRACTOR has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);

(j) The steps CONTRACTOR has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Event or Breach;

(k) Identify, describe or estimate the Persons, Workforce, Subcontractor, or Individuals and any law enforcement that may be involved in the Event or Breach;

(l) A reasonable schedule for CONTRACTOR to provide regular updates during normal business hours to the foregoing in the future for response to the Event or Breach, but no less than every three (3) business days or as otherwise directed by HHS, including information about risk estimations, reporting, notification, if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and

(m) Any reasonably available, pertinent information, documents or reports related to an Event or Breach that HHS requests following Discovery.

4.02 Investigation, Response and Mitigation. 45 CFR 164.308, 310 and 312; 164.530

(A) CONTRACTOR will immediately conduct a full and complete investigation, respond to the Event or Breach, commit necessary and appropriate staff and resources to

expeditiously respond, and report as required to and by HHS for incident response purposes and for purposes of HHS's compliance with report and notification requirements, to the reasonable satisfaction of HHS.

(B) CONTRACTOR will complete or participate in a risk assessment as directed by HHS following an Event or Breach, and provide the final assessment, corrective actions and mitigations to HHS for review and approval.

(C) CONTRACTOR will fully cooperate with HHS to respond to inquiries and/or proceedings by state and federal authorities, Persons and/or Individuals about the Event or Breach.

(D) CONTRACTOR will fully cooperate with HHS's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such Event or Breach, or to recover or protect any Confidential Information, including complying with reasonable corrective action or measures, as specified by HHS in a Corrective Action Plan if directed by HHS under the Base Contract.

4.03 Breach Notification to Individuals and Reporting to Authorities. Tex. Bus. & Comm. Code §521.053; 45 CFR 164.404 (Individuals), 164.406 (Media); 164.408 (Authorities)

(A) HHS may direct CONTRACTOR to provide Breach notification to Individuals, regulators or third-parties, as specified by HHS following a Breach.

(B) CONTRACTOR shall give HHS an opportunity to review and provide feedback to CONTRACTOR and to confirm that CONTRACTOR's notice meets all regulatory requirements regarding the time, manner and content of any notification to Individuals, regulators or third-parties, or any notice required by other state or federal authorities, including without limitation, notifications required by Texas Business and Commerce Code, Chapter 521.053(b) and HIPAA. HHS shall have ten (10) business days to provide said feedback to CONTRACTOR. Notice letters will be in CONTRACTOR's name and on CONTRACTOR's letterhead, unless otherwise directed by HHS, and will contain contact information, including the name and title of CONTRACTOR's representative, an email address and a toll-free telephone number, if required by applicable law, rule, or regulation, for the Individual to obtain additional information.

(C) CONTRACTOR will provide HHS with copies of distributed and approved communications.

(D) CONTRACTOR will have the burden of demonstrating to the reasonable satisfaction of HHS that any notification required by HHS was timely made. If there are delays outside of CONTRACTOR's control, CONTRACTOR will provide written documentation of the reasons for the delay.

(E) If HHS delegates notice requirements to CONTRACTOR, HHS shall, in the time and manner reasonably requested by CONTRACTOR, cooperate and assist with CONTRACTOR's information requests in order to make such notifications and reports.

ARTICLE 5.
STATEMENT OF WORK

"Statement of Work" means the services and deliverables to be performed or provided by CONTRACTOR, or on behalf of CONTRACTOR by its Subcontractors or agents for HHS that are described in detail in the Base Contract. The Statement of Work, including any future amendments thereto, is incorporated by reference in this DUA as if set out word-for-word herein.

ARTICLE 6.
GENERAL PROVISIONS

6.01 Oversight of Confidential Information

CONTRACTOR acknowledges and agrees that HHS is entitled to oversee and monitor CONTRACTOR's access to and creation, receipt, maintenance, use, disclosure of the Confidential Information to confirm that CONTRACTOR is in compliance with this DUA.

6.02 HHS Commitment and Obligations

HHS will not request CONTRACTOR to create, maintain, transmit, use or disclose PHI in any manner that would not be permissible under applicable law if done by HHS.

6.03 HHS Right to Inspection

At any time upon reasonable notice to CONTRACTOR, or if HHS determines that CONTRACTOR has violated this DUA, HHS, directly or through its agent, will have the right to inspect the facilities, systems, books and records of CONTRACTOR to monitor compliance with this DUA. For purposes of this subsection, HHS's agent(s) include, without limitation, the HHS Office of the Inspector General or the Office of the Attorney General of Texas, outside consultants or legal counsel or other designee.

6.04 Term; Termination of DUA; Survival

This DUA will be effective on the date on which CONTRACTOR executes the DUA, and will terminate upon termination of the Base Contract and as set forth herein. If the Base Contract is extended or amended, this DUA shall be extended or amended concurrent with such extension or amendment.

(A) HHS may immediately terminate this DUA and Base Contract upon a material violation of this DUA.

(B) Termination or Expiration of this DUA will not relieve CONTRACTOR of its obligation to return or Destroy the Confidential Information as set forth in this DUA and to continue to safeguard the Confidential Information until such time as determined by HHS.

(C) If HHS determines that CONTRACTOR has violated a material term of this DUA; HHS may in its sole discretion:

(1) Exercise any of its rights including but not limited to reports, access and inspection under this DUA and/or the Base Contract; or

(2) Require CONTRACTOR to submit to a Corrective Action Plan, including a plan for monitoring and plan for reporting, as HHS may determine necessary to maintain compliance with this DUA; or

(3) Provide CONTRACTOR with a reasonable period to cure the violation as determined by HHS; or

(4) Terminate the DUA and Base Contract immediately, and seek relief in a court of competent jurisdiction in Texas.

Before exercising any of these options, HHS will provide written notice to CONTRACTOR describing the violation, the requested corrective action CONTRACTOR may take to cure the alleged violation, and the action HHS intends to take if the alleged violated is not timely cured by CONTRACTOR.

(D) If neither termination nor cure is feasible, HHS shall report the violation to the Secretary of the U.S. Department of Health and Human Services.

(E) The duties of CONTRACTOR or its Subcontractor under this DUA survive the expiration or termination of this DUA until all the Confidential Information is Destroyed or returned to HHS, as required by this DUA.

6.05 Governing Law, Venue and Litigation

(A) The validity, construction and performance of this DUA and the legal relations among the Parties to this DUA will be governed by and construed in accordance with the laws of the State of Texas.

(B) The Parties agree that the courts of Texas, will be the exclusive venue for any litigation, special proceeding or other proceeding as between the parties that may be brought, or arise out of, or in connection with, or by reason of this DUA.

6.06 Injunctive Relief

(A) CONTRACTOR acknowledges and agrees that HHS may suffer irreparable injury if CONTRACTOR or its Subcontractor fails to comply with any of the terms of this

DUA with respect to the Confidential Information or a provision of HIPAA or other laws or regulations applicable to Confidential Information.

(B) CONTRACTOR further agrees that monetary damages may be inadequate to compensate HHS for CONTRACTOR's or its Subcontractor's failure to comply. Accordingly, CONTRACTOR agrees that HHS will, in addition to any other remedies available to it at law or in equity, be entitled to seek injunctive relief without posting a bond and without the necessity of demonstrating actual damages, to enforce the terms of this DUA.

6.07 Responsibility.

To the extent permitted by the Texas Constitution, laws and rules, and without waiving any immunities or defenses available to CONTRACTOR as a governmental entity, CONTRACTOR shall be solely responsible for its own acts and omissions and the acts and omissions of its employees, directors, officers, Subcontractors and agents. HHS shall be solely responsible for its own acts and omissions.

6.08 Insurance

(A) As a governmental entity, and in accordance with the limits of the Texas Tort Claims Act, Chapter 101 of the Texas Civil Practice and Remedies Code, CONTRACTOR either maintains commercial insurance or self-insures with policy limits in an amount sufficient to cover CONTRACTOR's liability arising under this DUA. CONTRACTOR will request that HHS be named as an additional insured. HHSC reserves the right to consider alternative means for CONTRACTOR to satisfy CONTRACTOR's financial responsibility under this DUA. Nothing herein shall relieve CONTRACTOR of its financial obligations set forth in this DUA if CONTRACTOR fails to maintain insurance.

(B) CONTRACTOR will provide HHS with written proof that required insurance coverage is in effect, at the request of HHS.

6.08 Fees and Costs

Except as otherwise specified in this DUA or the Base Contract, if any legal action or other proceeding is brought for the enforcement of this DUA, or because of an alleged dispute, contract violation, Event, Breach, default, misrepresentation, or injunctive action, in connection with any of the provisions of this DUA, each party will bear their own legal expenses and the other cost incurred in that action or proceeding.

6.09 Entirety of the Contract

This DUA is incorporated by reference into the Base Contract as an amendment thereto and, together with the Base Contract, constitutes the entire agreement between the parties. No change, waiver, or discharge of obligations arising under those documents will be valid unless in writing and executed by the party against whom such change, waiver, or discharge is sought to be enforced. If any provision of the Base Contract, including any General Provisions or Uniform Terms and Conditions, conflicts with this DUA, this DUA controls.

6.10 Automatic Amendment and Interpretation

If there is (i) a change in any law, regulation or rule, state or federal, applicable to HIPPA and/or Confidential Information, or (ii) any change in the judicial or administrative interpretation of any such law, regulation or rule,, upon the effective date of such change, this DUA shall be deemed to have been automatically amended, interpreted and read so that the obligations imposed on HHS and/or CONTRACTOR remain in compliance with such changes. Any ambiguity in this DUA will be resolved in favor of a meaning that permits HHS and CONTRACTOR to comply with HIPAA or any other law applicable to Confidential Information.

TEXAS Health and Human Services

Texas HHS System - Data Use Agreement - Attachment 2
SECURITY AND PRIVACY INQUIRY (SPI)

If you are a bidder for a new procurement/contract, in order to participate in the bidding process, you must have corrected any "No" responses (except A9a) prior to the contract award date. If you are an applicant for an open enrollment, you must have corrected any "No" answers (except A9a and A11) prior to performing any work on behalf of any Texas HHS agency.

For any questions answered "No" (except A9a and A11), an *Action Plan for Compliance with a Timeline* must be documented in the designated area below the question. The timeline for compliance with HIPAA-related requirements for safeguarding Protected Health Information is 30 calendar days from the date this form is signed. Compliance with requirements related to other types of Confidential Information must be confirmed within 90 calendar days from the date the form is signed.

SECTION A: APPLICANT/BIDDER INFORMATION (To be completed by Applicant/Bidder)

1. Does the applicant/bidder access, create, disclose, receive, transmit, maintain, or store Texas HHS Confidential Information in electronic systems (e.g., laptop, personal use computer, mobile device, database, server, etc.)? **IF NO, STOP. THE SPI FORM IS NOT REQUIRED.**	(●) Yes ( ) No
2. Entity or Applicant/Bidder Legal Name	Legal Name: COLLIN COUNTY GOVERNMENT Legal Entity Tax Identification Number (TIN) (Last Four Numbers Only): 6029 Procurement/Contract#: HHS000436300030 Address: 825 N MCDONALD ST. STE #145 City: MCKINNEY State: TX ZIP: 75069 Telephone #: (972) 548-5500 Email Address:
3. Number of Employees, at all locations, in Applicant/Bidder's Workforce "Workforce" means all employees, volunteers, trainees, and other Persons whose conduct is under the direct control of Applicant/Bidder, whether or not they are paid by Applicant/ Bidder. If Applicant/Bidder is a sole proprietor, the workforce may be only one employee.	Total Employees: 91
4. Number of Subcontractors (if Applicant/Bidder will not use subcontractors, enter "0")	Total Subcontractors: 1
5. Name of Information Technology Security Official and Name of Privacy Official for Applicant/Bidder (Privacy and Security Official may be the same person.)	**A. Security Official:** Legal Name: Jeff Springfield Address: 2300 Bloomdale Rd City: McKinney State: TX ZIP: 75071 Telephone #: (214) 862-6293 Email Address: jspringfield@co.collin.tx.us
	B. Privacy Official: Legal Name: CANDY BLAIR, CCHCS ADMINISTRATOR Address: 825 N MCDONALD ST. STE #145 City: MCKINNEY State: TX ZIP: 75069 Telephone #: (972) 548-5504 Email Address: CBLAIR@CO.COLLIN.TX.US

6. **Type(s) of Texas HHS Confidential Information the Applicant/Bidder will create, receive, maintain, use, disclose or have access to: (Check all that apply)** • *Health Insurance Portability and Accountability Act (HIPAA) data* • *Criminal Justice Information Services (CJIS) data* • *Internal Revenue Service Federal Tax Information (IRS FTI) data* • *Centers for Medicare & Medicaid Services (CMS)* • *Social Security Administration (SSA)* • *Personally Identifiable Information (PII)*	HIPAA ☑	CJIS ☐	IRS FTI ☐	CMS ☐	SSA ☐	PII ☑
	Other (Please List)					

7. **Number of Storage Devices for Texas HHS Confidential Information (as defined in the Texas HHS System Data Use Agreement (DUA))** Cloud Services involve using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. A Data Center is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.	Total # (Sum a-d) 167
a. Devices. Number of personal user computers, devices or drives, including mobile devices and mobile drives.	162
b. Servers. Number of Servers that are not in a data center or using Cloud Services.	3
c. Cloud Services. Number of Cloud Services in use.	1
d. Data Centers. Number of Data Centers in use.	1
8. Number of unduplicated individuals for whom Applicant/Bidder reasonably expects to handle Texas HHS Confidential Information during one year:	Select Option (a-d)
a. 499 individuals or less **b.** 500 to 999 individuals **c.** 1,000 to 99,999 individuals **d.** 100,000 individuals or more	○ a. ○ b. ◉ c. ○ d.
9. HIPAA Business Associate Agreement	
a. Will Applicant/Bidder use, disclose, create, receive, transmit or maintain protected health information on behalf of a HIPAA-covered Texas HHS agency for a HIPAA-covered function?	◉ Yes ○ No
b. Does Applicant/Bidder have a Privacy Notice prominently displayed on a Webpage or a Public Office of Applicant/Bidder's business open to or that serves the public? (This is a HIPAA requirement. Answer "N/A" if not applicable, such as for agencies not covered by HIPAA.)	◉ Yes ○ No ○ N/A
Action Plan for Compliance with a Timeline:	Compliance Date:
10. Subcontractors. If the Applicant/Bidder responded "0" to Question 4 (indicating no subcontractors), check "N/A" for both 'a.' and 'b.'	
a. Does Applicant/Bidder require subcontractors to execute the DUA Attachment 1 Subcontractor Agreement Form?	◉ Yes ○ No ○ N/A
Action Plan for Compliance with a Timeline:	Compliance Date:

b. Will Applicant/Bidder agree to require subcontractors who will access Confidential Information to comply with the terms of the DUA, not disclose any Confidential Information to them until they have agreed in writing to the same safeguards and to discontinue their access to the Confidential Information if they fail to comply?	(●) Yes ( ) No ( ) N/A
Action Plan for Compliance with a Timeline:	Compliance Date:
11. Does Applicant/Bidder have any **Optional Insurance** currently in place? Optional Insurance provides coverage for: (1) Network Security and Privacy; (2) Data Breach; (3) Cyber Liability (lost data, lost use or delay/suspension in business, denial of service with e-business, the Internet, networks and informational assets, such as privacy, intellectual property, virus transmission, extortion, sabotage or web activities); (4) Electronic Media Liability; (5) Crime/Theft; (6) Advertising Injury and Personal Injury Liability; and (7) Crisis Management and Notification Expense Coverage.	(●) Yes ( ) No ( ) N/A

SECTION B: PRIVACY RISK ANALYSIS AND ASSESSMENT (To be completed by Applicant/Bidder)

For any questions answered "No," an Action Plan for Compliance with a Timeline must be documented in the designated area below the question. The timeline for compliance with HIPAA-related requirements for safeguarding Protected Health Information is 30 calendar days from the date this form is signed. Compliance with requirements related to other types of Confidential Information must be confirmed within 90 calendar days from the date the form is signed.

1. Written Policies & Procedures. Does Applicant/Bidder have current written privacy and security policies and procedures that, at a minimum:	**Yes or No**
a. Does Applicant/Bidder have current written privacy and security policies and procedures that identify Authorized Users and Authorized Purposes (as defined in the DUA) relating to creation, receipt, maintenance, use, disclosure, access or transmission of Texas HHS Confidential Information?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
b. Does Applicant/Bidder have current written privacy and security policies and procedures that require Applicant/Bidder and its Workforce to comply with the applicable provisions of HIPAA and other laws referenced in the DUA, relating to creation, receipt, maintenance, use, disclosure, access or transmission of Texas HHS Confidential Information on behalf of a Texas HHS agency?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
c. Does Applicant/Bidder have current written privacy and security policies and procedures that limit use or disclosure of Texas HHS Confidential Information to the minimum that is necessary to fulfill the Authorized Purposes?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
d. Does Applicant/Bidder have current written privacy and security policies and procedures that respond to an actual or suspected breach of Texas HHS Confidential Information, to include at a minimum (if any responses are "No" check "No" for all three): i. Immediate breach notification to the Texas HHS agency, regulatory authorities, and other required Individuals or Authorities, in accordance with Article 4 of the DUA; ii. Following a documented breach response plan, in accordance with the DUA and applicable law; & iii. Notifying Individuals and Reporting Authorities whose Texas HHS Confidential Information has been breached, as directed by the Texas HHS agency?	◉ Yes ○ No

Action Plan for Compliance with a Timeline:	Compliance Date:
e. Does Applicant/Bidder have current written privacy and security policies and procedures that conduct annual workforce training and monitoring for and correction of any training delinquencies?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
f. Does Applicant/Bidder have current written privacy and security policies and procedures that permit or deny individual rights of access, and amendment or correction, when appropriate?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
g. Does Applicant/Bidder have current written privacy and security policies and procedures that permit only Authorized Users with up-to-date privacy and security training, and with a reasonable and demonstrable need to use, disclose, create, receive, maintain, access or transmit the Texas HHS Confidential Information, to carry out an obligation under the DUA for an Authorized Purpose, unless otherwise approved in writing by a Texas HHS agency?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
h. Does Applicant/Bidder have current written privacy and security policies and procedures that establish, implement and maintain proof of appropriate sanctions against any Workforce or Subcontractors who fail to comply with an Authorized Purpose or who is not an Authorized User, and used or disclosed Texas HHS Confidential Information in violation of the DUA, the Base Contract or applicable law?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
i. Does Applicant/Bidder have current written privacy and security policies and procedures that require updates to policies, procedures and plans following major changes with use or disclosure of Texas HHS Confidential Information within 60 days of identification of a need for update?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

j. Does Applicant/Bidder have current written privacy and security policies and procedures that restrict permissions or attempts to re-identify or further identify de-identified Texas HHS Confidential Information, or attempt to contact any Individuals whose records are contained in the Texas HHS Confidential Information, except for an Authorized Purpose, without express written authorization from a Texas HHS agency or as expressly permitted by the Base Contract?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
k. If Applicant/Bidder intends to use, disclose, create, maintain, store or transmit Texas HHS Confidential Information outside of the United States, will Applicant/Bidder obtain the express prior written permission from the Texas HHS agency and comply with the Texas HHS agency conditions for safeguarding offshore Texas HHS Confidential Information?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
l. Does Applicant/Bidder have current written privacy and security policies and procedures that require cooperation with Texas HHS agencies' or federal regulatory inspections, audits or investigations related to compliance with the DUA or applicable law?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
m. Does Applicant/Bidder have current written privacy and security policies and procedures that require appropriate standards and methods to destroy or dispose of Texas HHS Confidential Information?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
n. Does Applicant/Bidder have current written privacy and security policies and procedures that prohibit disclosure of Applicant/Bidder's work product done on behalf of Texas HHS pursuant to the DUA, or to publish Texas HHS Confidential Information without express prior approval of the Texas HHS agency?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
2. Does Applicant/Bidder have a current Workforce training program? Training of Workforce must occur at least once every year, and within 30 days of date of hiring a new Workforce member who will handle Texas HHS Confidential Information. Training must include: (1) privacy and security policies, procedures, plans and applicable requirements for handling Texas HHS Confidential Information, (2) a requirement to complete training before access is given to Texas HHS Confidential Information, and (3) written proof of training and a procedure for monitoring timely completion of training.	◉ Yes ○ No

Action Plan for Compliance with a Timeline:	Compliance Date:
3. Does Applicant/Bidder have Privacy Safeguards to protect Texas HHS Confidential Information in oral, paper and/or electronic form? "Privacy Safeguards" means protection of Texas HHS Confidential Information by establishing, implementing and maintaining required Administrative, Physical and Technical policies, procedures, processes and controls, required by the DUA, HIPAA (45 CFR 164.530), Social Security Administration, Medicaid and laws, rules or regulations, as applicable. Administrative safeguards include administrative protections, policies and procedures for matters such as training, provision of access, termination, and review of safeguards, incident management, disaster recovery plans, and contract provisions. Technical safeguards include technical protections, policies and procedures, such as passwords, logging, emergencies, how paper is faxed or mailed, and electronic protections such as encryption of data. Physical safeguards include physical protections, policies and procedures, such as locks, keys, physical access, physical storage and trash.	(●) Yes ( ) No
Action Plan for Compliance with a Timeline:	Compliance Date:
4. Does Applicant/Bidder and all subcontractors (if applicable) maintain a current list of Authorized Users who have access to Texas HHS Confidential Information, whether oral, written or electronic?	(●) Yes ( ) No
Action Plan for Compliance with a Timeline:	Compliance Date:
5. Does Applicant/Bidder and all subcontractors (if applicable) monitor for and remove terminated employees or those no longer authorized to handle Texas HHS Confidential Information from the list of Authorized Users?	(●) Yes ( ) No
Action Plan for Compliance with a Timeline:	Compliance Date:

SECTION C: SECURITY RISK ANALYSIS AND ASSESSMENT (to be completed by Applicant/Bidder)

This section is about your electronic system. If your business DOES NOT store, access, or transmit Texas HHS Confidential Information in electronic systems (e.g., laptop, personal use computer, mobile device, database, server, etc.) select the box to the right, and "YES" will be entered for all questions in this section.	**No Electronic Systems** ☐

For any questions answered "No," an Action Plan for Compliance with a Timeline must be documented in the designated area below the question. The timeline for compliance with HIPAA-related items is 30 calendar days, PII-related items is 90 calendar days.

1. Does the Applicant/Bidder ensure that services which access, create, disclose, receive, transmit, maintain, or store Texas HHS Confidential Information are maintained **IN** the United States (no offshoring) unless **ALL** of the following requirements are met? **a.** The data is encrypted with FIPS 140-2 validated encryption **b.** The offshore provider does not have access to the encryption keys **c.** The Applicant/Bidder maintains the encryption key within the United States **d.** The Application/Bidder has obtained the express prior written permission of the Texas HHS agency *For more information regarding FIPS 140-2 encryption products, please refer to:* *http://csrc.nist.gov/publications/fips*	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
2. Does Applicant/Bidder utilize an IT security-knowledgeable person or company to maintain or oversee the configurations of Applicant/Bidder's computing systems and devices?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
3. Does Applicant/Bidder monitor and manage access to Texas HHS Confidential Information (e.g., a formal process exists for granting access and validating the need for users to access Texas HHS Confidential Information, and access is limited to Authorized Users)?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
4. Does Applicant/Bidder a) have a system for changing default passwords, b) require user password changes at least every 90 calendar days, and c) prohibit the creation of weak passwords (e.g., require a minimum of 8 characters with a combination of uppercase, lowercase, special characters, and numerals, where possible) for all computer systems that access or store Texas HHS Confidential Information. **If yes, upon request must provide evidence such as a screen shot or a system report.**	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

5. Does each member of Applicant/Bidder's Workforce who will use, disclose, create, receive, transmit or maintain Texas HHS Confidential Information have a unique user name (account) and private password?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
6. Does Applicant/Bidder lock the password after a certain number of failed attempts and after 15 minutes of user inactivity in all computing devices that access or store Texas HHS Confidential Information?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
7. Does Applicant/Bidder secure, manage and encrypt remote access (including wireless access) to computer systems containing Texas HHS Confidential Information? (e.g., a formal process exists for granting access and validating the need for users to remotely access Texas HHS Confidential Information, and remote access is limited to Authorized Users). *Encryption is required for all Texas HHS Confidential Information. Additionally, **FIPS 140-2** validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.* *For more information regarding FIPS 140-2 encryption products, please refer to:* *http://csrc.nist.gov/publications/fips*	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
8. Does Applicant/Bidder implement computer security configurations or settings for all computers and systems that access or store Texas HHS Confidential Information? (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit exploitation opportunities for hackers or intruders, etc.)	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
9. Does Applicant/Bidder secure physical access to computer, paper, or other systems containing Texas HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.)?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

10. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information that is *transmitted* over a public network (e.g., the Internet, WiFi, etc.)? **If yes, upon request must provide evidence such as a screen shot or a system report.** *Encryption is required for all HHS Confidential Information. Additionally, **FIPS 140-2** validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.* *For more information regarding FIPS 140-2 encryption products, please refer to:* *http://csrc.nist.gov/publications/fips*	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
11. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information *stored* on end user devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.)? **If yes, upon request must provide evidence such as a screen shot or a system report.** *Encryption is required for all Texas HHS Confidential Information. Additionally, **FIPS 140-2** validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.* *For more information regarding FIPS 140-2 encryption products, please refer to:* *http://csrc.nist.gov/publications/fips*	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
12. Does Applicant/Bidder require Workforce members to formally acknowledge rules outlining their responsibilities for protecting Texas HHS Confidential Information and associated systems containing HHS Confidential Information before their access is provided?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
13. Is Applicant/Bidder willing to perform or submit to a criminal background check on Authorized Users?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
14. Does Applicant/Bidder prohibit the access, creation, disclosure, reception, transmission, maintenance, and storage of Texas HHS Confidential Information with a subcontractor (e.g., cloud services, social media, etc.) unless Texas HHS has approved the subcontractor agreement which must include compliance and liability clauses with the same requirements as the Applicant/Bidder?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

15. Does Applicant/Bidder keep current on security updates/patches (including firmware, software and applications) for computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information?	(●) Yes ( ) No
Action Plan for Compliance with a Timeline:	Compliance Date:
16. Do Applicant/Bidder's computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information contain up-to-date anti-malware and antivirus protection?	(●) Yes ( ) No
Action Plan for Compliance with a Timeline:	Compliance Date:
17. Does the Applicant/Bidder review system security logs on computing systems that access or store Texas HHS Confidential Information for abnormal activity or security concerns on a regular basis?	(●) Yes ( ) No
Action Plan for Compliance with a Timeline:	Compliance Date:
18. Notwithstanding records retention requirements, does Applicant/Bidder's disposal processes for Texas HHS Confidential Information ensure that Texas HHS Confidential Information is destroyed so that it is unreadable or undecipherable?	(●) Yes ( ) No
Action Plan for Compliance with a Timeline:	Compliance Date:
19. Does the Applicant/Bidder ensure that all public facing websites and mobile applications containing Texas HHS Confidential Information meet security testing standards set forth within the Texas Government Code (TGC), Section 2054.516; including requirements for implementing vulnerability and penetration testing and addressing identified vulnerabilities? *For more information regarding TGC, Section 2054.516 DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS, please refer to: https://legiscan.com/TX/text/HB8/2017*	(●) Yes ( ) No
Action Plan for Compliance with a Timeline:	Compliance Date:

SECTION D: SIGNATURE AND SUBMISSION (to be completed by Applicant/Bidder)

Please sign the form digitally, if possible. If you can't, provide a handwritten signature.

1. I certify that all of the information provided in this form is truthful and correct to the best of my knowledge. If I learn that any such information was not correct, I agree to notify Texas HHS of this immediately.

2. Signature	**3.** Title	**4.** Date:
Candy Blair	Public Health Director	3/3/23

To **submit** the completed, signed form:

- Email the form as an attachment to the appropriate Texas HHS Contract Manager(s).

Section E: To Be Completed by Texas HHS Agency Staff:

Agency(s): HHSC: ☐ DFPS: ☐ DSHS: ☒	Requesting Department(s): Department of State Health Services
Legal Entity Tax Identification Number (TIN) (Last four Only): [redacted] 6 4 3 2	PO/Contract(s) #: HHS001472800001

Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Gretchen Wells	Gretchen.Wells@dshs.texas.gov	(512) 776-2679
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:

INSTRUCTIONS FOR COMPLETING THE SECURITY AND PRIVACY INQUIRY (SPI)

Below are instructions for Applicants, Bidders and Contractors for Texas Health and Human Services requiring the Attachment 2, Security and Privacy Inquiry (SPI) to the Data Use Agreement (DUA). Instruction item numbers below correspond to sections on the SPI form.

If you are a bidder for a new procurement/contract, in order to participate in the bidding process, you must have corrected any "No" responses (except A9a) prior to the contract award date. If you are an applicant for an open enrollment, you must have corrected any "No" answers (except A9a and A11) prior to performing any work on behalf of any Texas HHS agency.

For any questions answered "No" (except A9a and A11), an *Action Plan for Compliance with a Timeline* must be documented in the designated area below the question. The timeline for compliance with HIPAA-related requirements for safeguarding Protected Health Information is 30 calendar days from the date this form is signed. Compliance with requirements related to other types of Confidential Information must be confirmed within 90 calendar days from the date the form is signed.

SECTION A. APPLICANT /BIDDER INFORMATION

Item #1. *Only contractors that access, transmit, store, and/or maintain Texas HHS Confidential Information will complete and email this form as an attachment to the appropriate Texas HHS Contract Manager.*

Item #2. Entity or Applicant/Bidder Legal Name. *Provide the legal name of the business (the name used for legal purposes, like filing a federal or state tax form on behalf of the business, and is not a trade or assumed named "dba"), the legal tax identification number (last four numbers only) of the entity or applicant/bidder, the address of the corporate or main branch of the business, the telephone number where the business can be contacted regarding questions related to the information on this form and the website of the business, if a website exists.*

Item #3. Number of Employees, at all locations, in Applicant/Bidder's workforce. *Provide the total number of individuals, including volunteers, subcontractors, trainees, and other persons who work for the business. If you are the only employee, please answer "1."*

Item #4. Number of Subcontractors. *Provide the total number of subcontractors working for the business. If you have none, please answer "0" zero.*

Item #5. Number of unduplicated individuals for whom Applicant/Bidder reasonably expects to handle HHS Confidential Information during one year. *Select the radio button that corresponds with the number of clients/consumers for whom you expect to handle Texas HHS Confidential Information during a year. Only count clients/consumers once, no matter how many direct services the client receives during a year.*

Item #5. Name of Information Technology Security Official and Name of Privacy Official for Applicant/Bidder. *As with all other fields on the SPI, this is a required field. This may be the same person and the owner of the business if such person has the security and privacy knowledge that is required to implement the requirements of the DUA and respond to questions related to the SPI. In 4.A. provide the name, address, telephone number, and email address of the person whom you have designated to answer any security questions found in Section C and in 4.B. provide this information for the person whom you have designated as the person to answer any privacy questions found in Section B. The business may contract out for this expertise; however, designated individual(s) must have knowledge of the business's devices, systems and methods for use, disclosure, creation, receipt, transmission and maintenance of Texas HHS Confidential Information and be willing to be the point of contact for privacy and security questions.*

Item #6. Type(s) of HHS Confidential Information the Entity or Applicant/Bidder Will Create, Receive, Maintain, Use, Disclose or Have Access to: *Provide a complete listing of all Texas HHS Confidential Information that the Contractor will create, receive, maintain, use, disclose or have access to. The DUA section Article 2, Definitions, defines Texas HHS Confidential Information as:*

> *"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to CONTRACTOR or that CONTRACTOR may create, receive, maintain, use, disclose or have access to on behalf of Texas HHS that consists of or includes any or all of the following:*
>
> *(1) Client Information;*
> *(2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information;*
> *(3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;*

(4) Federal Tax Information;
(5) Personally Identifiable Information;
(6) Social Security Administration Data, including, without limitation, Medicaid information;
(7) All privileged work product;
(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

Definitions for the following types of confidential information can be found the following sites:

- *Health Insurance Portability and Accountability Act (HIPAA) - http://www.hhs.gov/hipaa/index.html*
- *Criminal Justice Information Services (CJIS) - https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center*
- *Internal Revenue Service Federal Tax Information (IRS FTI) - https://www.irs.gov/pub/irs-pdf/p1075.pdf*
- *Centers for Medicare & Medicaid Services (CMS) - https://www.cms.gov/Regulations-and-Guidance/Regulations-and-Guidance.html*
- *Social Security Administration (SSA) - https://www.ssa.gov/regulations/*
- *Personally Identifiable Information (PII) - http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf*

Item #7. Number of Storage devices for Texas HHS Confidential Information. *The total number of devices is automatically calculated by exiting the fields in lines a - d. Use the <Tab> key when exiting the field to prompt calculation, if it doesn't otherwise sum correctly.*

- ***Item 7a. Devices****. Provide the number of personal user computers, devices, and drives (including mobile devices, laptops, USB drives, and external drives) on which your business stores or will store Texas HHS Confidential Information.*
- ***Item 7b. Servers****. Provide the number of servers not housed in a data center or "in the cloud," on which Texas HHS Confidential Information is stored or will be stored. A server is a dedicated computer that provides data or services to other computers. It may provide services or data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet. If none, answer "0" (zero).*
- ***Item 7c. Cloud Services****. Provide the number of cloud services to which Texas HHS Confidential Information is stored. Cloud Services involve using a network of remote servers hosted on the Internet to store, manage, and process data, rather than on a local server or a personal computer. If none, answer "0" (zero.)*
- ***Item 7d. Data Centers.*** *Provide the number of data centers in which you store Texas HHS Confidential Information. A Data Center is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. If none, answer "0" (zero).*

Item #8. Number of unduplicated individuals for whom the Applicant/Bidder reasonably expects to handle Texas HHS Confidential Information during one year*. Select the radio button that corresponds with the number of clients/consumers for whom you expect to handle Confidential Information during a year. Only count clients/consumers once, no matter how many direct services the client receives during a year.*

Item #9. HIPAA Business Associate Agreement*.*

- ***Item #9a.*** *Answer "Yes" if your business will use, disclose, create, receive, transmit, or store information relating to a client/consumer's healthcare on behalf of the Department of State Health Services, the Department of Disability and Aging Services, or the Health and Human Services Commission for treatment, payment, or operation of Medicaid or Medicaid clients. If your contract does not include HIPAA covered information, respond "no." If "no," a compliance plan is not required.*
- ***Item #9b.*** *Answer "Yes" if your business has a notice of privacy practices (a document that explains how you protect and use a client/consumer's healthcare information) displayed either on a website (if one exists for your business) or in your place of business (if that location is open to clients/consumers or the public). If your contract does not include HIPAA covered information, respond "N/A."*

Item #10. Subcontractors*. If your business responded "0" to question 4 (number of subcontractors), Answer "N/A" to Items 10a and 10b to indicate not applicable.*

- ***Item #10a.*** *Answer "Yes" if your business requires that all subcontractors sign Attachment 1 of the DUA.*
- ***Item #10b.*** *Answer "Yes" if your business obtains Texas HHS approval before permitting subcontractors to handle Texas HHS Confidential Information on your business's behalf.*

Item #11. Optional Insurance. *Answer "yes" if applicant has optional insurance in place to provide coverage for a Breach or any*

other situations listed in this question. If you are not required to have this optional coverage, answer "N/A" A compliance plan is not required.

SECTION B. PRIVACY RISK ANALYSIS AND ASSESSMENT

Reasonable and appropriate written Privacy and Security policies and procedures are required, even for sole proprietors who are the only employee, to demonstrate how your business will safeguard Texas HHS Confidential Information and respond in the event of a Breach of Texas HHS Confidential Information. To ensure that your business is prepared, all of the items below must be addressed in your written Privacy and Security policies and procedures.

Item #1. Answer "Yes" if you have written policies in place for each of the areas (a-o).

- **Item #1a.** Answer "yes" if your business has written policies and procedures that identify everyone, including subcontractors, who are authorized to use Texas HHS Confidential Information. The policies and procedures should also identify the reason why these Authorized Users need to access the Texas HHS Confidential Information and this reason must align with the Authorized Purpose described in the Scope of Work or description of services in the Base Contract with the Texas HHS agency.
- **Item #1b.** Answer "Yes" if your business has written policies and procedures that require your employees (including yourself), your volunteers, your trainees, and any other persons whose work you direct, to comply with the requirements of HIPAA, if applicable, and other confidentiality laws as they relate to your handling of Texas HHS Confidential Information. Refer to the laws and rules that apply, including those referenced in the DUA and Scope of Work or description of services in the Base Contract.
- **Item #1c.** Answer "Yes" if your business has written policies and procedures that limit the Texas HHS Confidential Information you disclose to the minimum necessary for your workforce and subcontractors (if applicable) to perform the obligations described in the Scope of Work or service description in the Base Contract. (e.g., if a client/consumer's Social Security Number is not required for a workforce member to perform the obligations described in the Scope of Work or service description in the Base Contract, then the Social Security Number will not be given to them.) If you are the only employee for your business, policies and procedures must not include a request for, or use of, Texas HHS Confidential Information that is not required for performance of the services.
- **Item #1d.** Answer "Yes" if your business has written policies and procedures that explain how your business would respond to an actual or suspected breach of Texas HHS Confidential Information. The written policies and procedures, at a minimum, must include the three items below. If any response to the three items below are no, answer "no."
    - **Item #1di.** Answer "Yes" if your business has written policies and procedures that require your business to immediately notify Texas HHS, the Texas HHS Agency, regulatory authorities, or other required Individuals or Authorities of a Breach as described in Article 4, Section 4 of the DUA.
      Refer to Article 4, Section 4.01:

      Initial Notice of Breach *must be provided in accordance with Texas HHS and DUA requirements with as much information as possible about the Event/Breach and a name and contact who will serve as the single point of contact with HHS both on and off business hours. Time frames related to Initial Notice include:*
        - *within one hour of Discovery of an Event or Breach of Federal Tax Information, Social Security Administration Data, or Medicaid Client Information*
        - *within 24 hours of all other types of Texas HHS Confidential Information* ***48-hour Formal Notice*** *must be provided no later than 48 hours after Discovery for protected health information, sensitive personal information or other non-public information and must include applicable information as referenced in Section 4.01 (C) 2. of the DUA.*
    - **Item #1dii.** Answer "Yes" if your business has written policies and procedures require you to have and follow a written breach response plan as described in Article 4 Section 4.02 of the DUA.
    - **Item #1diii.** Answer "Yes" if your business has written policies and procedures require you to notify Reporting Authorities and Individuals whose Texas HHS Confidential Information has been breached as described in Article 4 Section 4.03 of the DUA.
- **Item #1e.** Answer "Yes" if your business has written policies and procedures requiring annual training of your entire workforce on matters related to confidentiality, privacy, and security, stressing the importance of promptly reporting any Event or Breach, outlines the process that you will use to require attendance and track completion for employees who failed to complete annual training.

- **Item #1f.** Answer "Yes" if your business has written policies and procedures requiring you to allow individuals (clients/consumers) to access their individual record of Texas HHS Confidential Information, and allow them to amend or correct that information, if applicable.
- **Item #1g.** Answer "Yes" if your business has written policies and procedures restricting access to Texas HHS Confidential Information to only persons who have been authorized and trained on how to handle Texas HHS Confidential Information
- **Item #1h.** Answer "Yes" if your business has written policies and procedures requiring sanctioning of any subcontractor, employee, trainee, volunteer, or anyone whose work you direct when they have accessed Texas HHS Confidential Information but are not authorized to do so, and that you have a method of proving that you have sanctioned such an individuals. If you are the only employee, you must demonstrate how you will document the noncompliance, update policies and procedures if needed, and seek additional training or education to prevent future occurrences.
- **Item #1i.** Answer "Yes" if your business has written policies and procedures requiring you to update your policies within 60 days after you have made changes to how you use or disclose Texas HHS Confidential Information.
- **Item #1j.** Answer "Yes" if your business has written policies and procedures requiring you to restrict attempts to take de-identified data and re-identify it or restrict any subcontractor, employee, trainee, volunteer, or anyone whose work you direct, from contacting any individuals for whom you have Texas HHS Confidential Information except to perform obligations under the contract, or with written permission from Texas HHS.
- **Item #1k.** Answer "Yes" if your business has written policies and procedures prohibiting you from using, disclosing, creating, maintaining, storing or transmitting Texas HHS Confidential Information outside of the United States.
- **Item #1l.** Answer "Yes" if your business has written policies and procedures requiring your business to cooperate with HHS agencies or federal regulatory entities for inspections, audits, or investigations related to compliance with the DUA or applicable law.
- **Item #1m.** Answer "Yes" if your business has written policies and procedures requiring your business to use appropriate standards and methods to destroy or dispose of Texas HHS Confidential Information. Policies and procedures should comply with Texas HHS requirements for retention of records and methods of disposal.
- **Item #1n.** Answer "Yes" if your business has written policies and procedures prohibiting the publication of the work you created or performed on behalf of Texas HHS pursuant to the DUA, or other Texas HHS Confidential Information, without express prior written approval of the HHS agency.

Item #2. Answer "Yes" if your business has a current training program that meets the requirements specified in the SPI for you, your employees, your subcontractors, your volunteers, your trainees, and any other persons under you direct supervision.

Item #3. Answer "Yes" if your business has privacy safeguards to protect Texas HHS Confidential Information as described in the SPI.

Item #4. Answer "Yes" if your business maintains current lists of persons in your workforce, including subcontractors (if applicable), who are authorized to access Texas HHS Confidential Information. If you are the only person with access to Texas HHS Confidential Information, please answer "yes."

Item #5. Answer "Yes" if your business and subcontractors (if applicable) monitor for and remove from the list of Authorized Users, members of the workforce who are terminated or are no longer authorized to handle Texas HHS Confidential Information. If you are the only one with access to Texas HHS Confidential Information, please answer "Yes."

SECTION C. SECURITY RISK ANALYSIS AND ASSESSMENT

This section is about your electronic systems. If you DO NOT store Texas HHS Confidential Information in electronic systems (e.g., laptop, personal computer, mobile device, database, server, etc.), select the "No Electronic Systems" box and respond "Yes" for all questions in this section.

Item #1. Answer "Yes" if your business does not "offshore" or use, disclose, create, receive, transmit or maintain Texas HHS Confidential Information outside of the United States. If you are not certain, contact your provider of technology services (application, cloud, data center, network, etc.) and request confirmation that they do not off-shore their data.

Item #2. Answer "Yes" if your business uses a person or company who is knowledgeable in IT security to maintain or oversee the configurations of your business's computing systems and devices. You may be that person, or you may hire someone who can provide that service for you.

Item #3. Answer "Yes" if your business monitors and manages access to Texas HHS Confidential Information (i.e., reviews systems to ensure that access is limited to Authorized Users; has formal processes for granting, validating, and reviews the need for remote access to Authorized Users to Texas HHS Confidential Information, etc.). If you are the only employee, answer "Yes" if you have implemented a process to periodically evaluate the need for accessing Texas HHS Confidential Information to fulfill your Authorized Purposes.

Item #4. Answer "Yes" if your business has implemented a system for changing the password a system initially assigns to the user (also known as the default password), and requires users to change their passwords at least every 90 days, and prohibits the creation of weak passwords for all computer systems that access or store Texas HHS Confidential Information (e.g., a strong password has a minimum of 8 characters with a combination of uppercase, lowercase, special characters, and numbers, where possible). If your business uses a Microsoft Windows system, refer to the Microsoft website on how to do this, see example:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy

Item #5. Answer "Yes" if your business assigns a unique user name and private password to each of your employees, your subcontractors, your volunteers, your trainees and any other persons under your direct control who will use, disclose, create, receive, transmit or maintain Texas HHS Confidential Information.

Item #6. Answer "Yes" if your business locks the access after a certain number of failed attempts to login and after 15 minutes of user inactivity on all computing devices that access or store Texas HHS Confidential Information. If your business uses a Microsoft Windows system, refer to the Microsoft website on how to do this, see example:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy

Item #7. Answer "Yes" if your business secures, manages, and encrypts remote access, such as: using Virtual Private Network (VPN) software on your home computer to access Texas HHS Confidential Information that resides on a computer system at a business location or, if you use wireless, ensuring that the wireless is secured using a password code. If you do not access systems remotely or over wireless, answer "Yes."

Item #8. Answer "Yes" if your business updates the computer security settings for all your computers and electronic systems that access or store Texas HHS Confidential Information to prevent hacking or breaches (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit opportunities for hackers or intruders to access your system). For example, Microsoft's Windows security checklist:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings

Item #9. Answer "Yes" if your business secures physical access to computer, paper, or other systems containing Texas HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.). If you are the only employee and use these practices for your business, answer "Yes."

Item #10. Answer "Yes" if your business uses encryption products to protect Texas HHS Confidential Information that is transmitted over a public network (e.g., the Internet, WIFI, etc.) or that is stored on a computer system that is physically or electronically accessible to the public (FIPS 140-2 validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.) For more information regarding FIPS 140-2 encryption products, please refer to: *http://csrc.nist.gov/publications/fips*).

Item #11. Answer "Yes" if your business stores Texas HHS Confidential Information on encrypted end-user electronic devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.) and can produce evidence of the encryption, such as, a screen shot or a system report (FIPS 140-2 encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data). For more information regarding FIPS 140-2 validated encryption products, please refer to: *http://csrc.nist.gov/publications/fips*). If you do not utilize end-user electronic devices for storing Texas HHS Confidential Information, answer "Yes."

Item #12. Answer "Yes" if your business requires employees, volunteers, trainees and other workforce members to sign a document that clearly outlines their responsibilities for protecting Texas HHS Confidential Information and associated systems containing Texas HHS Confidential Information before they can obtain access. If you are the only employee answer "Yes" if you have signed or are willing to sign the DUA, acknowledging your adherence to requirements and responsibilities.

Item #13. Answer "Yes" if your business is willing to perform a criminal background check on employees, subcontractors, volunteers, or trainees who access Texas HHS Confidential Information. If you are the only employee, answer "Yes" if you are willing to submit to a background check.

Item #14. Answer "Yes" if your business prohibits the access, creation, disclosure, reception, transmission, maintenance, and storage of Texas HHS Confidential Information on Cloud Services or social media sites if you use such services or sites, and there is a Texas HHS approved subcontractor agreement that includes compliance and liability clauses with the same requirements as the Applicant/Bidder. If you do not utilize Cloud Services or media sites for storing Texas HHS Confidential Information, answer "Yes."

Item #15. Answer "Yes" if your business keeps current on security updates/patches (including firmware, software and applications) for computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information. If you use a Microsoft Windows system, refer to the Microsoft website on how to ensure your system is automatically updating, see example:
https://portal.msrc.microsoft.com/en-us/

Item #16. Answer "Yes" if your business's computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information contain up-to-date anti-malware and antivirus protection. If you use a Microsoft Windows system, refer to the Microsoft website on how to ensure your system is automatically updating, see example:
https://docs.microsoft.com/en-us/windows/security/threat-protection/

Item #17. Answer "Yes" if your business reviews system security logs on computing systems that access or store Texas HHS Confidential Information for abnormal activity or security concerns on a regular basis. If you use a Microsoft Windows system, refer to the Microsoft website for ensuring your system is logging security events, see example:
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies

Item #18. Answer "Yes" if your business disposal processes for Texas HHS Confidential Information ensures that Texas HHS Confidential Information is destroyed so that it is unreadable or undecipherable. Simply deleting data or formatting the hard drive is not enough; ensure you use products that perform a secure disk wipe. Please see NIST SP 800-88 R1, *Guidelines for Media Sanitization* and the applicable laws and regulations for the information type for further guidance.

Item #19. Answer "Yes" if your business ensures that all public facing websites and mobile applications containing HHS Confidential Information meet security testing standards set forth within the Texas Government Code (TGC), Section 2054.516

SECTION D. SIGNATURE AND SUBMISSION

Click on the signature area to digitally sign the document. Email the form as an attachment to the appropriate Texas HHS Contract Manager.

ATTACHMENT B

ACCESS TO PUBLIC HEALTH DASHBOARDS

I. PURPOSE

DSHS will provide LHE access to public health dashboards and data visualizations created by DSHS for certain data sets maintained by DSHS. LHE may access de-identified data on these dashboards for LHE's jurisdiction for the purpose of providing essential public health services even if it does not have an agreement with DSHS to access identified data; and, upon DSHS approval, statewide views may also be made available on public health dashboards.

II. SPECIAL CONSIDERATIONS FOR THE USE OF PUBLIC HEALTH DASHBOARDS

a) Dashboards and other data visualizations, including exports of information from these dashboards and data visualizations, created by DSHS and shared with LHE, may contain potentially identifiable public health data.
b) To receive potentially identifiable public health data sets from the dashboard(s) and/or data visualizations, an agreement under the MOU for the sharing of said data sets is required prior to the sharing of potentially identifiable public health data.
c) Only individuals having access credentials provided by DSHS are authorized to access these dashboards and/or data visualizations.
d) At its sole discretion, DSHS may or may not suppress data on public health dashboards or other data visualizations shared with LHE.
e) LHE shall not make any attempt to use the data on the dashboard or data visualizations to identify a person represented on the dashboard.

III. LIST OF INDIVIDUALS ACCESSING PUBLIC HEALTH DASHBOARD

LHE shall comply with Section IV(A) of the MOU regarding authorized users, including submission of information and notification of change in authorized users, having access to the public health dashboards under this document.

IV. REPRESENTATIVES FOR PUBLIC HEALTH DASHBOARDS

The representatives authorized to administer activities for public health dashboards under this document on behalf of their respective Party are listed under Article VI, Designation of Representatives, of the MOU.

ATTACHMENT C

ACCESS TO VITAL EVENT DATA

I. PURPOSE

DSHS agrees to provide LHE access to certain confidential data and information extracted from designated birth, death, fetal death and/or linked birth-infant death ("BID") records maintained by DSHS. LHE may access the vital event data that occurred in Texas for all residents of LHE's jurisdiction and contiguous jurisdictions as approved by DSHS (see Article III, LHE Jurisdiction, of the Contract) for the purpose set forth in Section IV herein.

II. LEGAL AUTHORITY

In addition to Chapter 121 of the Texas Health and Safety Code, DSHS has legal authority under the following statutes and administrative rules to share the data described herein:

a) Section 191.051 of the Texas Health and Safety Code;
b) Rule 181.1(21) in Title 25 of the Texas Administrative Code; and
c) Section 1001.089(b) of the Texas Health and Safety Code.

III. DESCRIPTION OF VITAL EVENT DATA TO BE PROVIDED

DSHS will provide LHE with provisional and statistically locked data files via secure data exchange, according to the variables outlined in Exhibit 1, Exhibit 2, and Exhibit 3, which is/are attached hereto, incorporated herein, and made part of the MOU for all purposes. In BID files, variables provided include only those death certificate items identified in the birth and death checklists in the Exhibit(s) attached and are completed for death certificates. If provisional files are available, then variables provided include only those items identified in the Exhibit(s) that are available for provisional data.

A. DSHS will provide residence data compiled by the usual place of residence without regard to the demographic place where the event occurred within Texas. For births and fetal deaths, the mother's usual residence is used as the place of residence.

B. DSHS will provide access to vital event data and information according to the following schedule and conditions:
   1. Access to data files will be provided approximately thirty (30) calendar days after the effective date of this MOU, or if access to certain data is approved through an amendment, then (thirty) 30 calendar days from effective date of the respective amendment. These data files will consist of:
      - Birth: data for years 2005 through the latest year of available data, as defined in Exhibit 1;
      - Death: data for years 2006 through the latest year of available data, as defined in Exhibit 2;
      - Fetal Death: data for years 2006 through the latest year of available data, as defined in Exhibit 3; and
      - BID: data for years 2006 through the latest year of available data, as defined in the applicable exhibits.
   2. The standard data sets for birth, death, and fetal death will be provided to each LHE as defined in Exhibit 1, Exhibit 2, and Exhibit 3, respectively. The standard data sets may be updated at DSHS' sole discretion to add, delete, or modify data elements. DSHS

may periodically add descriptive or calculated variables based on these data elements.
3. Data will be automatically updated when the new data files are available.
4. Once DSHS has granted an LHE authorized user access, that individual shall have log in access to the data twenty-four hours a day, seven days a week.
5. Annual statistically locked data files will replace that year's provisional data.

IV. INTENDED USE OF VITAL EVENT DATA

To monitor and analyze incidences of diseases to improve public health in the community.

V. SPECIAL CONSIDERATIONS FOR THE USE OF VITAL EVENT DATA

Under no circumstances shall LHE utilize the data and information to identify, disclose, or discover information concerning the specific adoptions, paternity determinations, or the identity of the parents of children who are the subjects of adoption placements. Any accidental identification of this information related to a child or parents of that child shall not be disclosed.

VI. LIST OF INDIVIDUALS ACCESSING DATA

In accordance with Section IV(A) of the MOU, LHE shall submit a list of staff names, titles, and email addresses in writing to the DSHS Representative identified in Section VII herein or through the DSHS identity and access management system, based upon guidance provided by DSHS. LHE shall notify DSHS Representatives of any changes in staff that require removal from the list of authorized users. Such notification must be made in writing or through DSHS' identity and access management system within five (5) business days of any staffing changes. On an annual basis and as additionally requested by DSHS, LHE shall certify the list of authorized users in writing to the DSHS Representatives identified in this MOU or through DSHS' identity and access management system, based upon guidance provided by DSHS.

VII. VITAL EVENT DATA ATTACHMENTS

The following exhibits are attached to this vital event data document and is/are incorporated into this document for all purposes.

- Exhibit 1: Checklist for Birth Certificate Data 2005 and beyond
- Exhibit 2: Checklist for Death Certificate Data 2006 and beyond
- Exhibit 3: Checklist for Fetal Death Certificate Data 2006 and beyond

VIII. VITAL EVENT DATA REPRESENTATIVES

The following will act as the representatives authorized to administer activities for vital event data under this document on behalf of their respective Party.

DSHS Contract Management Section (CMS)	**DSHS Center for Health Statistics (CHS)**	**Collin County (LHE)**
Gretchen Wells Contract Manager 1100 W 49th Street, MC1990 Austin, Texas 78756 (512) 776-2679 Gretchen.Wells@dshs.texas.gov	Jason Lucas Branch Manager PO Box 149347, MC 1898 Austin, Texas 78714-9347 (512) 776-6439 HIRBRequests@dshs.texas.gov	Taylor Burton 825 N. McDonald #130 McKinney, Tx 75069 (972) 548-4464 tburton@co.collin.tx.us