

**INTERLOCAL COOPERATION CONTRACT  
DEPARTMENT OF STATE HEALTH SERVICES  
CONTRACT NO.**

The DEPARTMENT OF STATE HEALTH SERVICES (“DSHS” or “SYSTEM AGENCY”) and Brown County (“LOCAL GOVERNMENT”), each a “Party” and collectively the “Parties,” enter into the following contract for Local Government access to the Texas Electronic Vital Events Registrar (“TxEVER”) (the “Contract”) pursuant to the provisions of the “Interlocal Cooperation Act,” *Tex. Gov’t Code Chapter 791*.

**I. CONTRACT REPRESENTATIVES**

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

<b><u>DSHS</u></b>	<b><u>Local Government</u></b>
Name: Department of State Health Services	Name: Brown County
Attn: Contract Management Section	Attn: County Clerk
Address: 1100 W 49 <sup>th</sup> Street, MC-1990	Address: 200 S Broadway
City, State, and Zip: Austin, TX 78776-2679756	City, State, and Zip: Brownwood, Tx 76801
Contact Person: Gretchen Wells	Contact Person: Sharon Ferguson
Telephone: (512) 776-2679	Telephone: (325) 643-2594
E-Mail: Gretchen.wells@dshs.texas.gov	E-Mail: <b>sharon.ferguson@browncountytexas.org</b>
Agency Number: 537	

**II. STATEMENT OF SERVICES TO BE PROVIDED**

The Parties agree to cooperate to provide necessary and authorized services and resources in accordance with the terms of the Contract. Specific services provided are described in **ATTACHMENT A, STATEMENT OF WORK**.

**III. CONTRACT PERIOD AND RENEWAL**

The Contract is effective on the signature date of the latter of the Parties to sign the Contract and expires **August 31, 2027**, unless renewed, extended, or terminated pursuant to the terms and conditions of the Contract. DSHS, at its sole discretion, may renew the Contract for up to one (1) additional year for a maximum Contract term of 5 years. Notwithstanding the limitation in the preceding sentence, and with at least 30 calendar days’ advance written notice to Local Government, at the end of the initial term or any renewal period, DSHS, at its sole discretion, may extend the Contract as necessary to ensure continuity of service, for purposes of transition, or as otherwise determined by DSHS to serve the best interest of the state of Texas for up to 12 months,

DSHS Contract No.

Page 1 of 8

June 5, 2023

(Exhibit #8)

in one-month intervals, at the then-current Contract rate or rates (if applicable) as modified during the term of the Contract.

**IV. AMENDMENT**

The Parties to the Contract may modify the Contract only through the execution of a written amendment signed by both Parties.

**V. FEES AND PAYMENT FOR SERVICES**

All payments made by Local Government to DSHS in connection with the Contract, including the manner in which payments to DSHS by Local Government will be rendered, are stated in **ATTACHMENT C, STATEMENT OF WORK.**

**VI. NOTICE REQUIREMENTS**

- A. All notices given by Local Government shall be in writing, include the Contract number, comply with all terms and conditions of the Contract, and be delivered to DSHS's Contract Representative identified above.
- B. Local Government shall send legal notices to DSHS at the address below and provide a copy to DSHS's Contract Representative:

**Health and Human Services Commission  
Attn: Office of the Chief Counsel  
4601 W Guadalupe St. MC-1100  
Austin, Texas 78751**

*with copy to*

**Department of State Health Services  
Attn: Office of General Counsel  
1100 W. 49th Street, MC-1919  
Austin, TX 78756**

- C. DSHS shall send legal notices to Local Government at the address below:

**Brown County  
200 S Broadway  
Brownwood, Texas 76801  
(325) 643-2594  
[sharon.ferguson@browncountytexas.org](mailto:sharon.ferguson@browncountytexas.org)**

- D. Notices given by DSHS to Local Government may be emailed, mailed or sent by common carrier. Email notices shall be deemed delivered when sent by DSHS. Notices sent by mail shall be deemed delivered when deposited by DSHS in the United States mail, postage

- paid, certified, return receipt requested. Notices sent by common carrier shall be deemed delivered when deposited by DSHS with a common carrier, overnight, signature required.
- E. Notices given by Local Government to DSHS shall be deemed delivered when received by DSHS.
  - F. Either Party may change its Contract Representative or Legal Notice contact by providing written notice to the other Party.

## VII. CONTRACT DOCUMENTS

The following documents are incorporated by reference and made a part of the Contract for all purposes. In the event of a conflict, ambiguity, or inconsistency between the terms and conditions set forth in the documents that comprise the Contract, the controlling document shall be this Signature Document, then the remaining documents in the following list in the order stated:

**ATTACHMENT A: HHS DATA USE AGREEMENT - TACCHO;**  
**ATTACHMENT B: HHS CONTRACT AFFIRMATIONS (VERSION 2.2); and**  
**ATTACHMENT C: STATEMENT OF WORK.**

## VIII. MISCELLANEOUS TERMS AND CONDITIONS

- A. Exchange of Personal Identifying Information.** The Contract concerns the exchange of Confidential Information. Except as prohibited by applicable law or regulation, Local Government and DSHS may exchange such information in accordance with *Tex. Health and Safety Code* Chapter 191.
- B. Suspension of Services or Contract Termination.** Use of services under the Contract by Local Government for purposes inconsistent with the Contract or applicable law or regulation may result in suspension of services or termination of the Contract for cause by DSHS.
- C. Governing Law and Venue.** The Contract 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 Contract is fixed in any court of competent jurisdiction of Travis County, Texas, unless the specific venue is otherwise identified in a statute which directly names or otherwise identifies its applicability to DSHS.
- D. Confidentiality.** Local Government shall maintain as confidential and shall not disclose to third parties without DSHS's prior written consent, any DSHS information including but not limited to DSHS Data, DSHS's business activities, practices, systems, conditions, and services. This section shall survive termination or expiration of the Contract. This requirement must be included in all subcontracts awarded by Local Government. The Parties shall comply with all applicable state and federal laws relating to the privacy and confidentiality of data and records provided under the Contract, including, but not limited to, *Tex. Gov't Code* Section 552.115.
- E. Record Maintenance and Retention**
1. Local Government shall keep and maintain under GAAP or GASB, as applicable, full, true, and complete records necessary to fully disclose to DSHS, the Texas State Auditor's Office, the United States Government, and their authorized representatives sufficient information to determine compliance with the terms and

conditions of the Contract and all state and federal rules, regulations, and statutes.

2. Local Government shall maintain and retain legible copies of the Contract and all records relating to the performance of the Contract, including supporting fiscal documents adequate to ensure that claims for Contract funds are in accordance with applicable state of Texas requirements. These records shall be maintained and retained by Local Government for a minimum of seven (7) years after the Contract expiration date or seven (7) years after the completion of all audit, claim, litigation, or dispute matters involving the Contract are resolved, whichever is later.

**F. Dispute Resolution.** To the extent that *Tex. Gov't Code* Chapter 2260 is applicable to the Contract, the dispute resolution process provided for in Chapter 2260, and the related rules adopted by the Texas Attorney General pursuant to Chapter 2260, shall be used by DSHS and Local Government to attempt to resolve any claim for breach of contract made by Local Government that cannot be resolved in the ordinary course of business.

**G. Entire Agreement.** The Contract contains all the terms and conditions between DSHS and Local Government relating to the matters set forth herein and no prior or contemporaneous agreement or understanding pertaining to the same shall be of any force or effect.

**H. Force Majeure.** Neither Local Government nor DSHS shall be liable to the other for any delay in, or failure of performance of, any requirement included in the Contract 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.

#### **I. INDEMNIFICATION**

1. **TO THE EXTENT ALLOWED BY THE CONSTITUTION AND LAWS OF THE STATE OF TEXAS, LOCAL GOVERNMENT SHALL DEFEND, INDEMNIFY AND HOLD HARMLESS THE STATE OF TEXAS, DSHS, AND HHSC, 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 LOCAL GOVERNMENT OR ITS AGENTS, EMPLOYEES, SUBCONTRACTORS, ORDER FULFILLERS, OR SUPPLIERS OF SUBCONTRACTORS IN THE EXECUTION OR**

**PERFORMANCE OF THE CONTRACT AND ANY PURCHASE ORDERS ISSUED UNDER THE CONTRACT.**

2. **THIS PARAGRAPH IS NOT INTENDED TO AND WILL NOT BE CONSTRUED TO REQUIRE LOCAL GOVERNMENT TO INDEMNIFY OR HOLD HARMLESS THE STATE OF TEXAS, DSHS, OR HHSC FOR ANY CLAIMS OR LIABILITIES RESULTING FROM THE NEGLIGENT ACTS OR OMISSIONS OF THE STATE OF TEXAS, DSHS, OR HHSC OR ITS EMPLOYEES.**
3. **FOR THE AVOIDANCE OF DOUBT, NEITHER THE STATE OF TEXAS, DSHS, NOR HHSC SHALL INDEMNIFY LOCAL GOVERNMENT OR ANY OTHER ENTITY UNDER THE CONTRACT.**

**J. No Waiver of Sovereign Immunity.** Nothing in the Contract shall be construed as a waiver of DSHS's, HHSC's, or the state of Texas' sovereign immunity. Neither the Contract nor any action or inaction of DSHS shall constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies, or immunities available to the State of Texas, DSHS, or HHSC. The failure to enforce, or any delay in the enforcement of, any privileges, rights, defenses, remedies, or immunities available to the State of Texas, DSHS, or HHSC under the Contract or under applicable law or regulation shall not constitute a waiver of such privileges, rights, defenses, remedies, or immunities or be considered as a basis for estoppel. Neither the State of Texas, DSHS, nor HHSC waives any privileges, rights, defenses, or immunities available to the State of Texas, DSHS, or HHSC by entering into the Contract or by its conduct prior to or subsequent to entering into the Contract. Notwithstanding the forgoing, if Local Government is a state of Texas agency or department, district, authority, county, municipality, or other political subdivision of the state of Texas, then nothing in the Contract will be construed to abrogate any rights or affirmative defenses available to Local Government under doctrines of sovereign and official immunity.

**K. Severability.** If any provision of the Contract is construed to be illegal or invalid, the illegal or invalid provision shall be deemed stricken and deleted to the same extent and effect as if never incorporated, but all other provisions shall continue.

**L. Waiver.** The failure of either Party to object to or to take affirmative action with respect to any conduct of either Party which is in violation or breach of the terms of the Contract shall not be construed as a waiver of the violation or breach, or of any future violation or breach.

**M. Termination**

1. **Convenience.** Either Party may terminate the Contract without cause by giving 30 days' written notice of its intent to terminate to the non-terminating Party. The termination will be effective on the date specified in the terminating Party's notice of termination.

1. **Cause resulting from Material Breach.** Except as otherwise provided by the U.S. Bankruptcy Code, or any successor law, either Party may terminate the Contract, in whole or in part, upon the following condition:
  - i. **Material Breach**  
If a Party determines, in its sole discretion, the other Party has materially breached the Contract or has failed to adhere to any laws, ordinances, rules, regulations or orders of any public authority having jurisdiction and such violation prevents or substantially impairs performance of the other Party's duties under the Contract.
2. **Cause resulting from Failure to Maintain Financial Viability.** DSHS may terminate the Contract if, in its sole discretion, DSHS has a good faith belief that Local Government no longer maintains the financial viability to fully perform its obligations under the Contract.

## IX. CERTIFICATIONS

The undersigned contracting Parties certify that:

- A. The services specified above are necessary and essential for activities that are properly within the statutory functions and programs of each Party;
- B. Each Party executing the Contract on its behalf has full power and authority to enter into the Contract;
- C. The proposed arrangements serve the interest of efficient and economical administration of state and local government; and
- D. The services contracted for are not required by Section 21, Article XVI of the Constitution of Texas to be supplied under a contract awarded to the lowest responsible bidder.

DSHS further certifies that it has statutory authority to contract for the services described in the Contract under *Tex. Health and Safety Code* Chapter 191 and *Tex. Gov't Code* Chapter 791.

Local Government further certifies that it has statutory authority to contract for the services described in the Contract under *Tex. Health and Safety Code* Chapter 191 and *Tex. Gov't Code* Chapter 791.

**SIGNATURE PAGE FOLLOWS**

SIGNATURE PAGE FOR DSHS CONTRACT NO.

DEPARTMENT OF STATE HEALTH SERVICES

BROWN COUNTY

\_\_\_\_\_  
Signature

Manda Hall, MD

Printed Name

Associate Commissioner for Community Health  
Improvement

Title



Date

\_\_\_\_\_  
Signature

Shane Britton

Printed Name

County Judge

Title

Date

June 5, 2023





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)**

<p>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.)? <b>IF NO, STOP. THE SPI FORM IS NOT REQUIRED.</b></p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p>2. <b>Entity or Applicant/Bidder Legal Name</b></p>	<p>Legal Name: <u>Brown County</u>          Legal Entity Tax Identification Number (TIN) (Last Four Numbers Only): <u>0838</u>          Procurement/Contract#:          Address: <u>200 S. Broadway Ste 101</u>          City: <u>Brownwood</u> State: <u>TX</u> ZIP: <u>76801</u>          Telephone #: <u>325-643-2594</u>          Email Address: <u>sharon.ferguson@browncountytexas.org</u></p>
<p>3. <b>Number of Employees, at all locations, in Applicant/Bidder's Workforce</b>          "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.</p>	<p>Total Employees: <u>7</u></p>
<p>4. <b>Number of Subcontractors</b>          (if Applicant/Bidder will not use subcontractors, enter "0")</p>	<p>Total Subcontractors: <u>0</u></p>
<p>5. <b>Name of Information Technology Security Official and Name of Privacy Official for Applicant/Bidder</b>          (Privacy and Security Official may be the same person.)</p>	<p><b>A. Security Official:</b>          Legal Name: <u>Goldsmith Solutions</u>          Address: <u>P.O. Box 224984</u>          City: <u>Dallas</u> State: <u>TX</u> ZIP: <u>75222</u>          Telephone #: <u>1-800-448-3153</u>          Email Address: <u>sam@goldsmithsolutions.com</u></p> <p><b>B. Privacy Official:</b> <u>Sam Goldsmith</u>          Legal Name: <u>Goldsmith Solutions</u>          Address: <u>P.O. Box 224984</u>          City: <u>Dallas</u> State: <u>TX</u> ZIP: <u>75222</u>          Telephone #: <u>1-800-448-3153</u>          Email Address: <u>Sam@goldsmithsolutions.com</u></p>

June 5, 2023  
(Exhibit # 8a)

<p><b>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)</b></p> <ul style="list-style-type: none"> <li>• Health Insurance Portability and Accountability Act (HIPAA) data</li> <li>• Criminal Justice Information Services (CJIS) data</li> <li>• Internal Revenue Service Federal Tax Information (IRS FTI) data</li> <li>• Centers for Medicare &amp; Medicaid Services (CMS)</li> <li>• Social Security Administration (SSA)</li> <li>• Personally Identifiable Information (PII)</li> </ul>	<p>HIPAA <input type="checkbox"/></p>	<p>CJIS <input type="checkbox"/></p>	<p>IRS FTI <input type="checkbox"/></p>	<p>CMS <input type="checkbox"/></p>	<p>SSA <input type="checkbox"/></p>	<p>PII <input checked="" type="checkbox"/></p>
<p>Other (Please List)</p>						
<p><b>7. Number of Storage Devices for Texas HHS Confidential Information (as defined in the Texas HHS System Data Use Agreement (DUA))</b></p> <p>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.</p> <p>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.</p>	<p>Total # (Sum a-d)</p> <p>0</p>					
<p><b>a. Devices.</b> Number of personal user computers, devices or drives, including mobile devices and mobile drives.</p>	<p>7</p>					
<p><b>b. Servers.</b> Number of Servers that are not in a data center or using Cloud Services.</p>	<p>1</p>					
<p><b>c. Cloud Services.</b> Number of Cloud Services in use.</p>	<p>1</p>					
<p><b>d. Data Centers.</b> Number of Data Centers in use.</p>	<p>0</p>					
<p><b>8. Number of unduplicated individuals for whom Applicant/Bidder reasonably expects to handle Texas HHS Confidential Information during one year:</b></p>	<p>Select Option (a-d)</p>					
<p>a. 499 individuals or less b. 500 to 999 individuals c. 1,000 to 99,999 individuals d. 100,000 individuals or more</p>	<p><input checked="" type="radio"/> a. <input type="radio"/> b. <input type="radio"/> c. <input type="radio"/> d.</p>					
<p><b>9. HIPAA Business Associate Agreement</b></p>						
<p><b>a.</b> 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?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>					
<p><b>b.</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.)</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A</p>					
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>					
<p><b>10. Subcontractors.</b> If the Applicant/Bidder responded "0" to Question 4 (indicating no subcontractors), check "N/A" for both 'a.' and 'b.'</p>						
<p><b>a.</b> Does Applicant/Bidder require subcontractors to execute the DUA Attachment 1 Subcontractor Agreement Form?</p>	<p><input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> N/A</p>					
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>					

<p><b>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?</b></p>	<p> <input type="radio"/> Yes  <input type="radio"/> No  <input checked="" type="radio"/> N/A </p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>11. Does Applicant/Bidder have any <b>Optional Insurance</b> currently in place?</b></p> <p>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.</p>	<p> <input checked="" type="radio"/> Yes  <input type="radio"/> No  <input type="radio"/> N/A </p>

**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
<p>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?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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):</p> <ul style="list-style-type: none"> <li>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;</li> <li>ii. Following a documented breach response plan, in accordance with the DUA and applicable law; &amp;</li> <li>iii. Notifying Individuals and Reporting Authorities whose Texas HHS Confidential Information has been breached, as directed by the Texas HHS agency?</li> </ul>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>

<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<b>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?</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<b>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?</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<b>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?</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<b>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?</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<b>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?</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

<p><b>j.</b> 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?</p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>k.</b> 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?</p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>l.</b> 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?</p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>m.</b> 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?</p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>n.</b> 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?</p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>2.</b> 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.</p>	<input checked="" type="radio"/> Yes <input type="radio"/> No

<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p><b>3. Does Applicant/Bidder have Privacy Safeguards to protect Texas HHS Confidential Information in oral, paper and/or electronic form?</b></p> <p>"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.</p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p><b>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?</b></p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p><b>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?</b></p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

**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**

- Yes  
 No

*For more information regarding FIPS 140-2 encryption products, please refer to:  
<http://csrc.nist.gov/publications/fips>*

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.**

- Yes  
 No

**If yes, upon request must provide evidence such as a screen shot or a system report.**

Action Plan for Compliance with a Timeline:

Compliance Date:



<p>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?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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).</p> <p><i>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 &amp; Medicaid Services (CMS) data.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: <a href="http://csrc.nist.gov/publications/fips">http://csrc.nist.gov/publications/fips</a></i></p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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.)</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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.)?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>


<p><b>10. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information that is <u>transmitted</u> over a public network (e.g., the Internet, WiFi, etc.)?</b></p> <p><b>If yes, upon request must provide evidence such as a screen shot or a system report.</b>  <i>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 &amp; Medicaid Services (CMS) data.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to:  <a href="http://csrc.nist.gov/publications/fips">http://csrc.nist.gov/publications/fips</a></i></p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>11. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information <u>stored</u> on end user devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.)?</b></p> <p><b>If yes, upon request must provide evidence such as a screen shot or a system report.</b>  <i>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 &amp; Medicaid Services (CMS) data.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to:  <a href="http://csrc.nist.gov/publications/fips">http://csrc.nist.gov/publications/fips</a></i></p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>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?</b></p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>13. Is Applicant/Bidder willing to perform or submit to a criminal background check on Authorized Users?</b></p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>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?</b></p>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>

<p><b>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?</b></p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>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?</b></p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>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?</b></p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>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?</b></p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p><b>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?</b></p> <p><i>For more information regarding TGC, Section 2054.516 DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS, please refer to: <a href="https://legiscan.com/TX/text/HB8/2017">https://legiscan.com/TX/text/HB8/2017</a></i></p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>

**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.**

<b>2. Signature</b> 	<b>3. Title</b> Brown County Clerk	<b>4. Date:</b> 06-8-2023
---	---------------------------------------	------------------------------

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: <input type="checkbox"/> DFPS: <input type="checkbox"/> DSHS: <input type="checkbox"/>	Requesting Department(s):
--	---------------------------

Legal Entity Tax Identification Number (TIN) (Last four Only): <table border="1" style="width:100%; height: 20px; border-collapse: collapse;"> <tr> <td style="width:12.5%;"></td> <td style="width:12.5%;"></td> <td style="width:12.5%;"></td> <td style="width:12.5%;"></td> <td style="width:12.5%;"></td> <td style="width:12.5%;"></td> <td style="width:12.5%;"></td> <td style="width:12.5%;"></td> </tr> </table>									PO/Contract(s) #:

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 #: