MEMORANDUM OF UNDERSTANDING
BETWEEN
DEPARTMENT OF STATE HEALTH SERVICES
AND
HIDALGO COUNTY
DSHS CONTRACT NO. HHS001434900003

This Memorandum of Understanding ("MOU") is between the **DEPARTMENT OF STATE HEALTH SERVICES** ("DSHS") and **HIDALGO COUNTY, TEXAS,** by and through its **PUBLIC HEALTH DEPARTMENT** ("Data Recipient" or "Contractor") who are collectively referred to as the "Parties."

I. PURPOSE

The Texas Cancer Registry ("TCR"), a component of DSHS, is a statewide population-based registry that collects and maintains information on new cancer cases diagnosed and treated in Texas. In addition, the TCR shares cancer data and supports a wide variety of cancer research and studies. DSHS agrees to provide Data Recipient certain confidential data and information collected by the TCR for assessment of essential public health services including monitoring health status of individuals in the community and evaluating effectiveness of population-based health services with the goal of reducing cancer rates and risk factors for cancer. This MOU provides the Parties' roles and responsibilities regarding access and utilization of the data and information as set forth in the Attachments to this MOU.

II. TERM OF THE MOU

This MOU is effective upon the signature date of the latter of the Parties to sign this MOU and expires on December 31, 2030, unless terminated sooner in accordance with the terms of this MOU.

III. AUTHORITY

This MOU is authorized by and in compliance with the following Texas statutes:

A. Texas Health and Safety Code, Section 1001.089(b);
B. Texas Health and Safety Code, Section 121.002;
C. Texas Health and Safety Code, Chapter 82, Texas Cancer Incidence Reporting Act;
D. Texas Health and Safety Code, Chapter 181, Medical Records Privacy;
E. Texas Administrative Code, Title 25, Health Services, Chapter 91, Subchapter A (Cancer Registry); and
F. Texas Business and Commerce Code, Chapter 521, Unauthorized Use of Identifying Information.

IV. STATEMENT OF WORK

A. Contractor will:

1. Comply with all DSHS policies and procedures regarding access and utilization of the data and information provided by DSHS. Data access and usage shall be limited to appropriate business needs and disclosed only as expressly authorized in this MOU.
2. Access and receive confidential data and information in a secure, confidential manner in compliance with all applicable federal and state laws governing the protection of confidential information.
3. Use industry best practices to secure, protect and manage confidential data and information. If Contractor moves information from DSHS systems, Contactor assumes responsibility for the security and privacy of the exported information.
4. Access, use and disclose confidential data and information for essential public health services and in accordance with the limited purposes described in this MOU. For avoidance of doubt, and for the purposes of this MOU, "essential public health services" is defined as conducting data analysis to monitor the health status of individuals in the community and evaluate the effectiveness of population-based health services with the goal of reducing the cancer burden in the community.
5. Promptly provide written notice to DSHS of any access, use, or disclosure of the confidential data and information which violates the terms of this MOU or applicable law.
6. Complete **ATTACHMENT B, TCR CONFIDENTIAL DATA REQUEST FORM** and submit to DSHS for review and approval.
7. Complete **ATTACHMENT D, LIST OF INDIVIDUALS ACCESSING CANCER DATA** and submit to DSHS for review and approval. Contractor will:
   a. Maintain a list of authorized users with access to DSHS confidential data and information and upon written request by DSHS, provide the list of authorized users within five (5) business days;
   b. Notify the DSHS Representative identified in this MOU in writing of any changes in staff that require removal from the list of authorized users. Such notification must be made in writing within five (5) business days of any staffing change; and
   c. On an annual basis and as requested by DSHS, certify the list of authorized users in writing to the DSHS Representative identified in this MOU. DSHS reserves the right to deny any additions, subtractions, or revisions to this attachment.
8. Submit a written application to DSHS for any new or ad hoc use of the data and information not described in this MOU. New or ad hoc use of the data is not authorized until DSHS has provided Contractor with written approval, and written amendment to this MOU is executed by both Parties.
9. Ensure authorized user(s) retrieve DSHS approved confidential data files from the DSHS secure file transfer (SFTP) server.

10. Review the confidential data files received from DSHS to ensure data received matches the data requested in **ATTACHMENT B, TCR CONFIDENTIAL DATA REQUEST FORM,** including the variables and diagnosis years cited.
11. Ensure all data and information provided by DSHS under this MOU, including data and information residing on back-up systems, remains within the contiguous United States and such data shall not be accessed by individuals located outside the contiguous United States. Furthermore, data and information may not be received, stored, processed, or disposed via information technology systems located outside of the contiguous United States.

B. DSHS will:

1. Provide each approved Contractor user with access credentials including the secure site, username, and password, as appropriate for rights to download the requested confidential data and information. This information will be provided directly to the Contractor staff member authorized to access the DSHS SFTP server.
2. Deliver the confidential data file via SFTP and notify Contractor, through notice to Contractor's authorized user, that the requested data file is available on the DSHS SFTP server so that Contractor's authorized user may retrieve the data file promptly.
3. Subject to DSHS' receipt and approval of completed **ATTACHMENT D, LIST OF INDIVIDUALS ACCESSING CANCER DATA**, and **ATTACHMENT B, TCR CONFIDENTIAL DATA REQUEST FORM**, deliver the requested confidential data file within 60 calendar days of the effective date of this MOU.
4. Deliver any subsequent confidential data files requested by Contractor within 60 calendar days of a new diagnosis year being available and following receipt of and approval by DSHS of updated **ATTACHMENT B, TCR CONFIDENTIAL DATA REQUEST FORM** and **ATTACHMENT D, LIST OF INDIVIDUALS ACCESSING CANCER DATA**.
5. Remove user access to the DSHS SFTP as requested by Contractor within five (5) business days of receipt of Contractor's written request.

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. GENERAL TERMS AND CONDITIONS

A. Amendment

This MOU may be modified by written amendment signed by the Parties.

B. Confidentiality

1. Contractor shall comply with all applicable state and federal laws relating to the privacy, security, and confidentiality of the confidential data and information

2. Contractor shall comply with the **HHS DATA USE AGREEMENT-TACCHO VERSION, OCTOBER 23, 2019** ("DUA") which is attached to and incorporated into this MOU as **ATTACHMENT A**.
3. Contractor will maintain appropriate procedural, administrative, physical and technical safeguards to prevent release or disclosure of any confidential data and information obtained under this MOU to anyone other than individuals who are authorized by law to receive such data or information and who will protect the data and information from re-disclosure as required by law. Data will be maintained in a secure location and in compliance with the DUA.
4. No personally identifiable information ("PII") and non-public data may be accessed or disclosed by Contractor without specific statutory authority and prior DSHS written approval. Only aggregate data resulting from analyses using data obtained under this MOU should appear in any report or publication (written, visual or sound). Rates and associated counts in any reports and publications containing aggregate data shall be suppressed when they are based on 1-10 cases. For maps, strategies to reduce geographic specificity shall be employed (e.g., offset precise locations, mask geographic areas with low case numbers, display ranges instead of exact values).
5. Contractor shall not attempt to link nor permit others to attempt to link the records of individuals in the data sets obtained under this MOU with personally identifiable data or records from any other source.
6. For avoidance of doubt, Contractor is expressly prohibited from using, and permitting any third party to use, DSHS data and information for marketing, research, or other non-governmental or commercial purposes without prior written consent of DSHS.
7. The proprietary nature of Contractor's systems that process, store, collect, and/or transmit the DSHS data shall not excuse Contractor's performance of its obligations hereunder.
8. All Contractor staff, representatives, or subcontractors granted access to systems managed by DSHS are required to review the **HHS INFORMATION SECURITY ACCEPTABLE USE POLICY** and sign the **HHS INFORMATION SECURITY ACCEPTABLE USE AGREEMENT,** attached hereto as **ATTACHMENT F** and **G** respectively, as a condition of their access.
9. Contractor shall destroy all data and information obtained under this MOU in a manner that renders the data unusable, unreadable or indecipherable to unauthorized individuals. Contractor shall destroy data files in accordance with the following schedule:
    a. Updated data files replace any previously obtained data files. The previous data files shall be destroyed within 60 calendar days of receipt of the updated data file.
    b. Upon destruction of the data files, Contractor shall complete and submit **ATTACHMENT C, TCR CERTIFICATE OF DATA DESTRUCTION**, within 30 calendar days of receipt of the updated data file.
    c. Under no circumstances shall Contractor retain data files after the expiration or termination of this MOU.

10. DSHS will cease data sharing immediately upon expiration or termination of this MOU.

C. Termination

The Parties agree that either Party may terminate this MOU for any reason.

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

D. Status of Parties

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

E. No Cost

This is a "no cost" agreement; the Contractor shall not be obligated to make any payments of any amount to DSHS or other parties as a result of this MOU. Any costs and expenses incurred under the terms of this MOU will be paid by the Party incurring the cost or expense. No funds appropriated to either Party will be exchanged under this MOU.

F. Counterparts and Signatures

The Parties may sign this MOU in counterparts, each of which will be deemed an original, but all of which together constitute one document. Electronically transmitted signatures will be deemed originals for all purposes related to this MOU.

G. Texas Public Information Act

Each Party is responsible for complying with the provisions of Texas Government Code Chapter 552 ("Texas Public Information Act") and the attorney general opinions issued under that statute. Responses to requests for information shall be handled in accordance with the provisions of the Texas Public Information Act.

H. Right to Audit

Contractor 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 Contractor pertaining to the MOU for purposes of inspecting, monitoring, auditing, or evaluating by DSHS and the State of Texas.

I. Assignment

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

J. 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; provided however, nothing in this paragraph shall preclude either Party from pursuing any remedies available under Texas law.

K. 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.

L. Severability

If any provision of this MOU is construed to be illegal or invalid, that provision will be deemed stricken to the same extent as if it was never an element of the MOU, but all other provisions will continue in effect.

M. No Waiver

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.

N. 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 this MOU is fixed in any court of competent jurisdiction of Travis County, Texas.

O. Survivability

Expiration or termination of the Contract for any reason does not release Data Recipient from any liability or obligation set forth in the Contract that is expressly stated to survive any such expiration or termination, 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 Contract, including without limitation

the provisions regarding warranty, indemnification, confidentiality, and rights and remedies upon termination.

P. 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.

Q. 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.

R. Limitation on Authority
Contractor 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. Contractor may not incur any debt, obligation, expense or liability of any kind on behalf of DSHS or the State of Texas.

S. 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.

VI. AUTHORIZED REPRESENTATIVES

The following individuals 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**	**Hidalgo County**
Maria Acuña, CTCM Contract Manager 1100 W 49th Street, MC1990 Austin, Texas 78756 (512) 776-6629 maria.acuna@dshs.texas.gov	Natalie Archer, CESB Director 1100 W 49th Street Austin, Texas 78756 (512) 776-6416 natalie.archer@dshs.texas.gov	Dairen Sarmiento Rangel Director, Department of Health & Human Services 1304 S. 25th Ave. Edinburg, Texas, 78542 (956) 383-6221 dairen.sarmiento@hchd.org

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:

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

Data Recipient
Hidalgo County Criminal District Attorney's Office
Attn: Toribio "Terry" Palacios
100 E. Cano 2nd Floor
Edinburg, TX 78539

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

Notice given in any other manner shall be deemed effective only when received by the Party to be notified.

Either Party may change its address for receiving legal notice by notifying the other Party in writing.

VIII. DOCUMENTS FORMING MOU

The following documents are attached and incorporated by reference and made a part of this MOU for all purposes:

ATTACHMENT A: HHS DATA USE AGREEMENT - TACCHO VERSION, OCTOBER. 23, 2019
ATTACHMENT B: TEXAS CANCER REGISTRY CONFIDENTIAL DATA REQUEST FORM
ATTACHMENT C: TEXAS CANCER REGISTRY CERTIFICATE OF DATA DESTRUCTION
ATTACHMENT D: LIST OF INDIVIDUALS ACCESSING CANCER DATA
ATTACHMENT E: HHS CONTRACT AFFIRMATIONS, VERSION 2.6 (JULY 2025)
ATTACHMENT F: HHS INFORMATION SECURITY ACCEPTABLE USE POLICY
ATTACHMENT G: HHS INFORMATION SECURITY ACCEPTABLE USE AGREEMENT

SIGNATURE PAGE FOLLOWS

SIGNATURE PAGE
DSHS Contract No. HHS001434900003

By signing below, the Parties agree that this MOU constitutes the entire agreement between them. The Parties acknowledge 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.

DEPARTMENT OF STATE HEALTH SERVICES	**HIDALGO COUNTY, TEXAS**
Signature of Authorized Official	Signature of Authorized Official
Manda Hall, MD Printed Name	Richard F. Cortez Printed Name
Associate Commissioner for Community Health Improvement Title	Hidalgo County Judge Title
Date	Date

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 or offered under Texas Government Code Sec. 2054.519(f).

(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: Hidalgo County Legal Entity Tax Identification Number (TIN) (Last Four Numbers Only): 7176 Procurement/Contract#: HHS001434900003 Address: 1304 S. 25th Ave City: Edinburg State: TX ZIP: 78542 Telephone #: (956) 383-6221 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: 200
4. Number of Subcontractors (if Applicant/Bidder will not use subcontractors, enter "0")	Total Subcontractors: 0
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: Daniel Salinas Address: 100 E. Cano, 4th Floor City: Edinburg State: TX ZIP: 78539 Telephone #: (956) 292-7010 Email Address: daniel.salinas@co.hidalgo.tx.us
	B. Privacy Official: Legal Name: Anayatzi Medina Address: 1304 S. 25th Ave City: Edinburg State: TX ZIP: 78542 Telephone #: (956) 383-6221 Email Address: anayatzi.medina@hchd.org

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) PHI and SPI					

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) 234
a. Devices. Number of personal user computers, devices or drives, including mobile devices and mobile drives.	215
b. Servers. Number of Servers that are not in a data center or using Cloud Services.	18
c. Cloud Services. Number of Cloud Services in use.	1
d. Data Centers. Number of Data Centers in use.	0

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 Up to five people will have access.	○ 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:
	Hidalgo County Judge	9/23/25

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):
Legal Entity Tax Identification Number (TIN) (Last four Only):	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 #:
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.

TEXAS Health and Human Services | Texas Department of State Health Services

Attachment B
Texas Cancer Registry
Confidential Data Request Form

Background: This form is to be used by entities requesting confidential Texas Cancer Registry data once it is determined the request does not require DSHS IRB review and approval. It should be attached to the required Memorandum of Understanding (MOU).

Instructions: Complete and return this form (including the Data Item Selection Table) to CancerData@dshs.texas.gov as a Word document (in DRAFT form).

Entity Requesting TCR Data	Hidalgo County Health & Human Services Department
Project Title	Hidalgo County TCR Data Request

Primary Contact					
Last Name	Gonzalez	*First Name*	Amy	*Degrees*	MPH
Title	Epidemiologist III – Lead Epidemiologist				
Mailing Address	1211 S. 28th Ave, Edinburg, TX 78542				
Phone Number	956-318-2426 ext. 7332	*Email*	amy.gonzalez@hchd.org		
Secondary Contact					
Last Name	Rocha	*First Name*	Savannah	*Degrees*	BS
Title	Epidemiologist I				
Mailing Address	1211 S. 28th Ave, Edinburg, TX 78542				
Phone Number	956-318-2426 ext. 7245	*Email*	savannah.rocha@hchd.org		

Summary Description of the Project
Provide a brief description of the project. Keep this section to one page (single-spaced). This section should focus on the aspect of your project that involves TCR data, including how TCR data will be used and why it is needed to achieve your study aims.
Primary Focus
Our primary focus for having access to this data would be to better understand our local cancer rates, track changes in data over time, and identify potential areas for targeted prevention initiatives.
Objectives
To utilize this data to apply for grants, community education campaigns, the development of local prevention strategies, and include the data in a chronic disease dashboard.
Methods (relevant to TCR data)
The data will be used for descriptive analysis, time series analysis, and quantitative analysis.

Data Analyses (state specifically how TCR data will be used in the analyses)

We will use the requested data to provide a broad overview of how cancer rates have changed over time within our jurisdiction. Descriptive analysis will be used to summarize the overall burden of cancer through measures such as case counts, crude rates, and age-adjusted rates across demographic groups. Time series analysis will be used to examine trends over multiple years to identify patterns or shifts in cancer rates and calculate population-based rates to support comparisons across groups and time periods.

Data Products Planned (e.g., internal or external presentation, manuscript, internal report)

Data will be used for internal report and analysis to create initiatives for targeted prevention initiatives, sharing general overall data to local stakeholders, and use statistical data for providing awareness through a chronic disease dashboard. The dashboard will display a general overview of cancer rates within our jurisdiction by year and by basic demographics, where available. Users will be able to view simple visualizations (e.g., bar graphs, trend lines) showing how rates have changed over time. No individual-level data will be included, and all data will be aggregated and de-identified.
Our vision for the chronic disease public-facing dashboard is to provide the rates of cancer within our population through statistical rates per 100,000. If after review of the data, the age breakdown information is not significant and representative of the data, we wouldn't include the information. Attached to this email, is a sample of how we would like to display information on rates in Hidalgo County for the chronic diseases we intend to focus on.

Data Selection Criteria

Sex

All (includes all available codes shown in the NAACCR Data Dictionary)

See all available codes for patient's sex in the NAACCR Data Dictionary

Years of Diagnosis

- The earliest available diagnosis year is 1995.
- It takes approximately two years after the close of a calendar year to collect, quality control, consolidate, and produce analysis files that are considered complete (defined as including at least 95% of all incident cancer cases among Texas residents in a given year).
- Studies requesting the most current information available will receive data that are incomplete and may not pass the CDC's National Program of Cancer Registries (NPCR), North American Association of Central Cancer Registries (NAACCR), and Surveillance, Epidemiology, and End Results (SEER) Program edit checks.
- Caution is warranted when analyzing 2020 diagnosis year data. See more information here: https://seer.cancer.gov/data/covid-impact.html

Begin: 1/1/2012 End: 12/31/2022

Age at Diagnosis

Age range: All ages

Geographic location at time of diagnosis (select one)

☐ All of Texas
☒ Specific location in Texas (counties): Hidalgo
☐ Specific location in Texas (zip codes):
☐ Specific location in Texas (census tracts):

☐ Specific location in Texas (other):

Cancer Sites (select one)
☒ All cancer sites
☐ Specific cancer sites/types

- List the cancer site groups you are requesting from the SEER Site Recode ICD-O-3/WHO 2008 definitions:
- If the requested study population is entirely children and adolescents (less than 20 years of age), the International Classification of Childhood Cancer (ICCC) Recode ICD-O-3/WHO 2008 is recommended, but not required. This classification includes benign, borderline, and malignant tumors (behaviors 0, 1, and 3, respectively). If ICCC is used, list the specific extended classification recodes:
- If SEER site and ICCC-3 recodes do not apply, list the specific ICD-O-3 topographical codes (site) and morphology codes (histology):

Behavior (select all that apply)
☒ Invasive/malignant cancers
☒ *In situ* cancers
☒ Benign/borderline (where reportable)

Additional Selection Criteria (e.g., limiting dataset by race/ethnicity or stage at diagnosis)

Data Item Selection

- Use the table below to select all data items being requested.
  - Only data items checked or added to the table will be provided. More rows can be inserted as needed at the bottom of the table.
- Only select data items relevant to your project. The TCR and IRB reviews applications from the perspective of minimum release of data necessary to accomplish aims.
- Data items marked with an asterisk require specific justification in the table below and in your protocol.
- Confidential data items are in bold. These items require specific justification in the table below and in your protocol.
- Please review the TCR Data Dictionary and NAACCR Data Dictionary before selecting data items and submitting the application.
  - Data items will be labeled using the XML NAACCR ID, when available.
  - The numbers shown within brackets next to each data item name is the NAACCR item number in the NAACCR Data Dictionary. Not all data items have NAACCR item numbers.

Dataset Format
Preferred file format for dataset: Excel (.xlsx)

	TCR Data Item [NAACCR #] Only select data items relevant to your study.	**Years Available**	**Justification/More Information** *Justification required for data items with an asterisk.
Patient Demographics			
☒	Patient ID Number [20] Sequence Number—Central [380] Tumor Record Number [60] CTC ID (unique tumor identifier)	1995-current	Included in all datasets
☒	Sex [220]	1995-current	
☒	Race/Ethnicity Recode	1995-current	Mutually exclusive categories, as follows: Hispanic; Non-Hispanic American Indian/Alaska Native (AI/AN); Non-Hispanic Asian/Pacific Islander (A/PI); Non-Hispanic Black; Non-Hispanic White; Other/Unknown.

TCR Data Item [NAACCR #] Only select data items relevant to your study.	Years Available	Justification/More Information *Justification required for data items with an asterisk.
☐ Race 1 [160]	1995-current	
☐ Race 2 [161]	1995-current	
☐ Spanish/Hispanic Origin [190]	1995-current	
☐ NHIA Derived Hispanic Origin [191]	1995-current	
☐ Race-NAPIIA (Derived API) [193]	1995-current	
☐ **Date of Birth [240]*** *Choose YYYY, YYYYMM, or YYYYMMDD:* **Year only (YYYY)**	1995-current	Enter justification for YYYYMM or YYYYMMDD.
☐ Birthplace--State [252]*	2013-current	Caution Warranted – See TCR Data Dictionary
☐ Birthplace--Country [254]*	2013-current	Caution Warranted – See TCR Data Dictionary
☐ **Name--Last [2230]***	1995-current	
☐ **Name--First [2240]***	1995-current	
☐ **Name--Middle [2250]***	1995-current	
☐ **Name--Suffix [2270]***	2011-current	
☐ **Addr Current—No & Street [2350]*** **Addr Current—City [1810]*** **Addr Current—State [1820]*** **Addr Current—Postal Code [1830]***	1995-current	
☐ **Telephone [2360]***	1995-current	
Characteristics at Diagnosis		
☐ Addr at DX--State [80]	1995-current	
☐ County at DX Analysis [89]	1995-current	
☐ **Addr at DX—City [70]***	1995-current	
☐ **Addr at DX—No & Street [2330]***	1995-current	
☐ **Addr at DX—Postal Code [100]***	1995-current	

TCR Data Item [NAACCR #] Only select data items relevant to your study.	Years Available	Justification/More Information *Justification required for data items with an asterisk.
☒ Rural-Urban Continuum *Rural-Urban Continuum 1993 [3300]* *Rural-Urban Continuum 2003 [3310]* *Rural-Urban Continuum 2013 [3312]*	1995-current	
☒ **Census Tract 2000 [130]*** Census Tract Certainty 2000 [365]	1995-2009	Time series analysis
☒ **Census Tract 2010 [135]*** Census Tract Certainty 2010 [367]	2010-2019	Time series analysis
☒ **Census Tract 2020 [125]*** Census Tract Certainty 2020 [369]	2020-current	Time series analysis
☒ Census Tract Poverty Indicator [145]	1995-current	
☐ **Latitude [2352]*** **Longitude [2354]*** GIS Coordinate Quality [366]	1995-current	
☐ Texas Public Health Region	1995-current	
☐ Primary Payer at Diagnosis [630]*	2007-current	Caution Warranted – See TCR Data Dictionary
☐ **Date of Diagnosis [390]*** *Choose YYYY, YYYYMM, or YYYYMMDD:* **Year only (YYYY)**	1995-current	Enter justification for YYYYMM or YYYYMMDD.
☒ Age at Diagnosis [230]	1995-current	
☐ CoC Accredited Flag [2152]	2018-current	
Tumor Characteristics		
☒ Primary Site [400]	1995-current	
☐ Laterality [410]	1995-current	
☒ Diagnosis Confirmation [490]	1995-current	
☐ Type of Reporting Source [500]	1995-current	
☒ Histologic Type ICD-O-3 [522]	1995-current	
☒ Behavior Code ICD-O-3 [523]	1995-current	

TCR Data Item [NAACCR #] Only select data items relevant to your study.	**Years Available**	**Justification/More Information** *Justification required for data items with an asterisk.
☒ Site Recode ICD-O-3/WHO 2008	1995-current	
☒ International Classification of Childhood Cancer (ICCC) Recode ICD-O-3/WHO 2008 Extended Classification	1995-current	Cases diagnosed at <20 years of age. Because ICCC-3 includes benign and borderline tumors for certain site groups, ensure benign/borderline behavior is checked in "Data Selection Criteria" above, if requesting those site groups.
☒ Summary Stage Combined (one data item that includes the summary stage data item required for that year) [759, 760, 3020, 764, 762]	1995-current	
☐ Tumor Size Summary [756]	2016-current	
☐ EOD Tumor Size [780]	1995-2003	
☐ Collaborative Stage (CS)--Tumor Size [2800]	2004-2015	
☐ Regional Nodes Examined [830]	1998-current	
☐ Regional Nodes Positive [820]	1998-current	
☐ TNM Clinical Stage* *Diagnosis years 2015-2017:* - *TNM Clinical Stage [940, 950, 960, 970]** *Diagnosis years 2018-current:* - *TNM Clinical Stage [1001, 1002, 1003, 1004]**	2015-current	Caution Warranted – See TCR Data Dictionary
☐ TNM Pathologic Stage* *Diagnosis years 2015-2017:* - *TNM Pathologic Stage [880, 890, 900, 910]** *Diagnosis years 2018-current:* - *TNM Pathologic Stage [1011, 1012, 1013, 1014]**	2015-current	Caution Warranted – See TCR Data Dictionary
☐ TNM Edition Number [1060]*	2015-current	Caution Warranted – See TCR Data Dictionary
☐ CS--Extension [2810]	2004-2015	
☐ CS--Lymph Nodes [2830]	2004-2015	
☐ CS--Metastasis at Diagnosis [2850]	2004-2015	
☐ CS--Site Specific Factor 1 [2880]	2010-2017	
☐ CS--Site Specific Factor 2 [2890]	2010-2017	
☐ CS--Site Specific Factor 3 [2900]	2010-2015	

TCR Data Item [NAACCR #] Only select data items relevant to your study.	**Years Available**	**Justification/More Information** *Justification required for data items with an asterisk.
☐ CS--Site Specific Factor 15 [2869]	2011-2017	
☐ CS--Site Specific Factor 25 [2879]	2010-2017	
☐ Mets at Diagnosis *Mets at Diagnosis – Bone [1112]* *Mets at Diagnosis – Brain [1113]* *Mets at Diagnosis – Distant LNs [1114]* *Mets at Diagnosis – Liver [1115]* *Mets at Diagnosis – Lung [1116]* *Mets at Diagnosis – Other [1117]*	2022-current	
☐ Schema ID [3800]	2018-current	
☐ Brain Molecular Markers [3816]	2018-current	
☐ Breslow Tumor Thickness [3817]	2018-current	
☐ Estrogen Receptor Summary [3827]	2018-current	
☐ Fibrosis Score [3835]	2018-current	
☐ Grade *Diagnosis years 1995-2017:* - *Grade [440]* *Diagnosis years 2018-current:* - *Grade Clinical [3843]* - *Grade Pathological [3844]*	1995-current	Data Items provided may vary based on diagnosis years requested.
☐ HER2 Overall Summary [3855]	2018-current	
☐ Microsatellite Instability (MSI) [3890]	2018-current	
☐ Progesterone Receptor Summary [3915]	2018-current	
☐ PSA Lab Value [3920]	2018-current	
☐ Gleason Data Items *Gleason Patterns Clinical [3838]* *Gleason Patterns Pathological [3839]* *Gleason Score Clinical [3840]* *Gleason Score Pathological [3841]* *Gleason Tertiary Pattern [3842]*	2021-current	
☐ LDH Pretreatment Lab Value [3932]	2018-current	
First Course Treatment*		

TCR Data Item [NAACCR #] Only select data items relevant to your study.	**Years Available**	**Justification/More Information** *Justification required for data items with an asterisk.
TCR treatment data do not undergo the same quality assurance checks as other core data fields. Treatment data often are reported as available and tend to have a higher proportion of incomplete or missing information compared to diagnosis-related or other core data items. Treatment fields may have a value of "none" or "unknown," both of which do not necessarily indicate an absence of treatment. Therefore, **drawing conclusions about the effect of treatment on outcomes is not appropriate**. Treatment data may be used for exploratory or supplementary purposes only. Please describe how these important limitations of the treatment data will be incorporated into your study design and/or analysis. **Initial each item listed below if requesting treatment data items:** ____ I have reviewed and considered the limitations of the treatment-related data and will factor these limitations into the study design and/or analysis appropriately. ____ I understand that using TCR data to draw conclusions about the effect of treatment on outcomes is not appropriate.		**Provide justification here if any treatment data items are requested. Include a description of your plan for addressing missing or potentially inaccurate data.**
☐ **Treatment Initiation Date [1260]***	2010-current	
☐ Surgery of Primary Site 03-2022 [1290]*	1995-2022	
☐ Scope Regional Lymph Node Surgery [1292]*	2001-current	
☐ Surgical Removal of Distal Lymph Nodes or Other Tissue [1294] *	1998-current	
☐ Reason for No Surgery [1340]*	1998-2002; 2006-current	
☐ Type of Radiation Treatment [1360]*	1998–2002; 2012–2017	

TCR Data Item [NAACCR #] Only select data items relevant to your study.	**Years Available**	**Justification/More Information** *Justification required for data items with an asterisk.
☐ Dominant Modality of Radiation [1570]*	2003-2017	
☐ Reason for No Radiation [1430]*	1998–2002; 2011–current	
☐ Phase I Radiation Treatment Modality [1506]*	2018-current	
☐ Sequence of Radiation and Surgery [1380]*	2004-current	
☐ Chemotherapy [1390]*	1995-current	
☐ Hormone Therapy [1400]*	1995-current	
☐ Immunotherapy [1410]*	1995-current	
☐ Other Treatment (not surgery, radiation, or systemic therapy) [1420]*	1995-current	
☐ Hematologic Transplant and Endocrine Procedures [3250]*	2003-current	

Cause of Death and Follow-up		
☐ **Surv-Date Presumed Alive [1785]*** Surv-Flag Presumed Alive [1786] Surv-Months Presumed Alive [1787] **Surv-Date DX Recode [1788]*** Vital Status Recode [1762]	1995-current	Only available for survival analysis. Click to enter justification.
☐ **Date of Last Contact [1750]***	1995-current	
☐ Place of Death--State [1942]	1995-current	
☐ Place of Death--Country [1944]	1995-current	
☐ Vital Status [1760]	1995-current	
☐ Follow-Up Source Central [1791]	2006-current	
☐ Cause of Death [1910]* ICD Revision Number [1920]	1995-current	
Additional Data Items		
List any additional data items relevant for your study (e.g., birth surname and social security number for data linkage conducted by the TCR). **Enter the NAACCR data item number and justification.** These fields may not have undergone the same quality assurance checks as other core data fields and may have a high proportion of missing or incomplete information. (To add more rows, click the blue plus sign at the bottom right corner of the table.)		

TEXAS Health and Human Services | Texas Department of State Health Services

Attachment C
Texas Cancer Registry
Certificate of Data Destruction

Instructions: Complete this form to confirm data destruction for Texas Cancer Registry data provided through a DSHS MOU. Upon completion, submit to cancerdata@dshs.texas.gov.

1. DSHS MOU No.:

2. List the data that were destroyed:

3. List the software program(s) used for securely destroying the data and any copies, derivatives, subsets, and manipulated files, if applicable:

4. By signing this Certificate, I confirm that ALL data requested for the DSHS MOU listed above and as applicable, copies, derivatives, subsets and manipulated files, held by all individuals who had access to, and from all the computers/storage devices where the files were processed/stored have been properly destroyed.

MOU DATA RECIPIENT PROGRAM CONTACT:	
ORGANIZATION:	
EMAIL:	PHONE:
AUTHORIZED REPRESENTATIVE SIGNATURE:	DATE:

ATTACHMENT D
LIST OF INDIVIDUALS ACCESSING CANCER DATA

Name	Organization	E-mail	Phone

HEALTH AND HUMAN SERVICES
Contract Number HHS001434900003
Attachment E CONTRACT AFFIRMATIONS

For purposes of these Contract Affirmations, HHS includes both the Health and Human Services Commission (HHSC) and the Department of State Health Services (DSHS). System Agency refers to HHSC, DSHS, or both, that will be a party to this Contract. These Contract Affirmations apply to all Contractors and Grantees (referred to as "Contractor") regardless of their business form (e.g., individual, partnership, corporation).

By entering into this Contract, Contractor affirms, without exception, understands, and agrees to comply with the following items through the life of the Contract:

1. Contractor represents and warrants that these Contract Affirmations apply to Contractor and all of Contractor's principals, officers, directors, shareholders, partners, owners, agents, employees, subcontractors, independent contractors, and any other representatives who may provide services under, who have a financial interest in, or otherwise are interested in this Contract and any related Solicitation.

2. Complete and Accurate Information

Contractor represents and warrants that all statements and information provided to HHS are current, complete, and accurate. This includes all statements and information in this Contract and any related Solicitation Response.

3. Public Information Act

Contractor understands that HHS will comply with the Texas Public Information Act (Chapter 552 of the Texas Government Code) as interpreted by judicial rulings and opinions of the Attorney General of the State of Texas. Information, documentation, and other material prepared and submitted in connection with this Contract or any related Solicitation may be subject to public disclosure pursuant to the Texas Public Information Act. In accordance with Section 2252.907 of the Texas Government Code, Contractor is required to make any information created or exchanged with the State pursuant to the Contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the State.

4. Contracting Information Requirements

Contractor represents and warrants that it will comply with the requirements of Section 552.372(a) of the Texas Government Code. Except as provided by Section 552.374(c) of the Texas Government Code, the requirements of Subchapter J (Additional Provisions Related to Contracting Information), Chapter 552 of the Government Code, may apply to the Contract and the Contractor agrees that the Contract can be terminated if the Contractor knowingly or intentionally fails to comply with a requirement of that subchapter.

5. Assignment

A. Contractor shall not assign its rights under the Contract or delegate the performance of its duties under the Contract without prior written approval from System Agency. Any attempted assignment in violation of this provision is void and without effect.

B. Contractor understands and agrees the System Agency may in one or more transactions assign, pledge, or transfer the Contract. Upon receipt of System Agency's notice of assignment, pledge, or transfer, Contractor shall cooperate with System Agency in giving effect to such assignment, pledge, or transfer, at no cost to System Agency or to the recipient entity.

6. Terms and Conditions

Contractor accepts the Solicitation terms and conditions unless specifically noted by exceptions advanced in the form and manner directed in the Solicitation, if any, under which this Contract was awarded. Contractor agrees that all exceptions to the Solicitation, as well as terms and conditions advanced by Contractor that differ in any manner from HHS' terms and conditions, if any, are rejected unless expressly accepted by System Agency in writing.

7. HHS Right to Use

Contractor agrees that HHS has the right to use, produce, and distribute copies of and to disclose to HHS employees, agents, and contractors and other governmental entities all or part of this Contract or any related Solicitation Response as HHS deems necessary to complete the procurement process or comply with state or federal laws.

8. Release from Liability

Contractor generally releases from liability and waives all claims against any party providing information about the Contractor at the request of System Agency.

9. Dealings with Public Servants

Contractor has not given, has not offered to give, and does not intend to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with this Contract or any related Solicitation, or related Solicitation Response.

10. Financial Participation Prohibited

Under Section 2155.004, Texas Government Code (relating to financial participation in preparing solicitations), Contractor certifies that the individual or business entity named in this Contract and any related Solicitation Response is not ineligible to receive this Contract and acknowledges that this Contract may be terminated and payment withheld if this certification is inaccurate.

11. Prior Disaster Relief Contract Violation

Under Sections 2155.006 and 2261.053 of the Texas Government Code (relating to convictions and penalties regarding Hurricane Rita, Hurricane Katrina, and other disasters), the Contractor certifies that the individual or business entity named in this Contract and any related Solicitation Response is not ineligible to receive this Contract

and acknowledges that this Contract may be terminated and payment withheld if this certification is inaccurate.

12. Child Support Obligation

Under Section 231.006(d) of the Texas Family Code regarding child support, Contractor certifies that the individual or business entity named in this Contract and any related Solicitation Response is not ineligible to receive the specified payment and acknowledges that the Contract may be terminated and payment may be withheld if this certification is inaccurate. If the certification is shown to be false, Contractor may be liable for additional costs and damages set out in 231.006(f).

13. Suspension and Debarment

Contractor certifies that it and its principals are not suspended or debarred from doing business with the state or federal government as listed on the *State of Texas Debarred Vendor List* maintained by the Texas Comptroller of Public Accounts and the *System for Award Management (SAM*) maintained by the General Services Administration. This certification is made pursuant to the regulations implementing Executive Order 12549 and Executive Order 12689, Debarment and Suspension, 2 C.F.R. Part 376, and any relevant regulations promulgated by the Department or Agency funding this project. This provision shall be included in its entirety in Contractor's subcontracts, if any, if payment in whole or in part is from federal funds.

14. Excluded Parties

Contractor certifies that it is not listed in the prohibited vendors list authorized by Executive Order 13224, *"Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism,"* published by the United States Department of the Treasury, Office of Foreign Assets Control.'

15. Foreign Terrorist Organizations

Contractor represents and warrants that it is not engaged in business with Iran, Sudan, or a foreign terrorist organization, as prohibited by Section 2252.152 of the Texas Government Code.

16. Executive Head of a State Agency

In accordance with Section 669.003 of the Texas Government Code, relating to contracting with the executive head of a state agency, Contractor certifies that it is not (1) the executive head of an HHS agency, (2) a person who at any time during the four years before the date of this Contract was the executive head of an HHS agency, or (3) a person who employs a current or former executive head of an HHS agency.

17. Human Trafficking Prohibition

Under Section 2155.0061 of the Texas Government Code, Contractor certifies that the individual or business entity named in this Contract is not ineligible to receive this Contract and acknowledges that this Contract may be terminated and payment withheld if this certification is inaccurate.

18. Franchise Tax Status

Contractor represents and warrants that it is not currently delinquent in the payment of any franchise taxes owed the State of Texas under Chapter 171 of the Texas Tax Code.

19. Debts and Delinquencies

Contractor agrees that any payments due under this Contract shall be applied towards any debt or delinquency that is owed to the State of Texas.

20. Lobbying Prohibition

Contractor represents and warrants that payments to Contractor and Contractor's receipt of appropriated or other funds under this Contract or any related Solicitation are not prohibited by Sections 556.005, 556.0055, or 556.008 of the Texas Government Code (relating to use of appropriated money or state funds to employ or pay lobbyists, lobbying expenses, or influence legislation).

21. Buy Texas

Contractor agrees to comply with Section 2155.4441 of the Texas Government Code, requiring the purchase of products and materials produced in the State of Texas in performing service contracts.

22. Disaster Recovery Plan

Contractor agrees that upon request of System Agency, Contractor shall provide copies of its most recent business continuity and disaster recovery plans.

23. Computer Equipment Recycling Program

If this Contract is for the purchase or lease of computer equipment, then Contractor certifies that it is in compliance with Subchapter Y, Chapter 361 of the Texas Health and Safety Code related to the Computer Equipment Recycling Program and the Texas Commission on Environmental Quality rules in 30 TAC Chapter 328.

24. Television Equipment Recycling Program

If this Contract is for the purchase or lease of covered television equipment, then Contractor certifies that it is compliance with Subchapter Z, Chapter 361 of the Texas Health and Safety Code related to the Television Equipment Recycling Program.

25. Cybersecurity Training

A. Contractor represents and warrants that it will comply with the requirements of Section 2054.5192 of the Texas Government Code relating to cybersecurity training and required verification of completion of the training program.

B. Contractor represents and warrants that if Contractor or Subcontractors, officers, or employees of Contractor have access to any state computer system or database, the Contractor, Subcontractors, officers, and employees of Contractor shall complete cybersecurity training pursuant to and in accordance with Government Code, Section 2054.5192.

26. Restricted Employment for Certain State Personnel

Contractor acknowledges that, pursuant to Section 572.069 of the Texas Government Code, a former state officer or employee of a state agency who during the period of state service or employment participated on behalf of a state agency in a procurement or contract negotiation involving Contractor may not accept employment from Contractor before the second anniversary of the date the Contract is signed or the procurement is terminated or withdrawn.

27. No Conflicts of Interest

A. Contractor represents and warrants that it has no actual or potential conflicts of interest in providing the requested goods or services to System Agency under this Contract or any related Solicitation and that Contractor's provision of the requested goods and/or services under this Contract and any related Solicitation will not constitute an actual or potential conflict of interest or reasonably create an appearance of impropriety.

B. Contractor agrees that, if after execution of the Contract, Contractor discovers or is made aware of a Conflict of Interest, Contractor will immediately and fully disclose such interest in writing to System Agency. In addition, Contractor will promptly and fully disclose any relationship that might be perceived or represented as a conflict after its discovery by Contractor or by System Agency as a potential conflict. System Agency reserves the right to make a final determination regarding the existence of Conflicts of Interest, and Contractor agrees to abide by System Agency's decision.

28. Fraud, Waste, and Abuse

Contractor understands that HHS does not tolerate any type of fraud, waste, or abuse. Violations of law, agency policies, or standards of ethical conduct will be investigated, and appropriate actions will be taken. Pursuant to Texas Government Code, Section 321.022, if the administrative head of a department or entity that is subject to audit by the state auditor has reasonable cause to believe that money received from the state by the department or entity or by a client or contractor of the department or entity may have been lost, misappropriated, or misused, or that other fraudulent or unlawful conduct has occurred in relation to the operation of the department or entity, the administrative head shall report the reason and basis for the belief to the Texas State Auditor's Office (SAO). All employees or contractors who have reasonable cause to believe that fraud, waste, or abuse has occurred (including misconduct by any HHS employee, Grantee officer, agent, employee, or subcontractor that would constitute fraud, waste, or abuse) are required to immediately report the questioned activity to the Health and Human Services Commission's Office of Inspector General. Contractor agrees to comply with all applicable laws, rules, regulations, and System Agency policies regarding fraud, waste, and abuse including, but not limited to, HHS Circular C-027.

A report to the SAO must be made through one of the following avenues:

- SAO Toll Free Hotline: 1-800-TX-AUDIT
- SAO website: http://sao.fraud.state.tx.us/

All reports made to the OIG must be made through one of the following avenues:

- OIG Toll Free Hotline 1-800-436-6184
- OIG Website: ReportTexasFraud.com
- Internal Affairs Email: InternalAffairsReferral@hhsc.state.tx.us
- OIG Hotline Email: OIGFraudHotline@hhsc.state.tx.us.
- OIG Mailing Address: Office of Inspector General
  Attn: Fraud Hotline
  MC 1300
  P.O. Box 85200
  Austin, Texas 78708-5200

29. Antitrust

The undersigned affirms under penalty of perjury of the laws of the State of Texas that:

A. in connection with this Contract and any related Solicitation Response, neither I nor any representative of the Contractor has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;

B. in connection with this Contract and any related Solicitation Response, neither I nor any representative of the Contractor has violated any federal antitrust law; and

C. neither I nor any representative of the Contractor has directly or indirectly communicated any of the contents of this Contract and any related Solicitation Response to a competitor of the Contractor or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Contractor.

30. Legal and Regulatory Actions

Contractor represents and warrants that it is not aware of and has received no notice of any court or governmental agency proceeding, investigation, or other action pending or threatened against Contractor or any of the individuals or entities included in numbered paragraph 1 of these Contract Affirmations within the five (5) calendar years immediately preceding execution of this Contract or the submission of any related Solicitation Response that would or could impair Contractor's performance under this Contract, relate to the contracted or similar goods or services, or otherwise be relevant to System Agency's consideration of entering into this Contract. If Contractor is unable to make the preceding representation and warranty, then Contractor instead represents and warrants that it has provided to System Agency a complete, detailed disclosure of any such court or governmental agency proceeding, investigation, or other action that would or could impair Contractor's performance under this Contract, relate to the contracted or similar goods or services, or otherwise be relevant to System Agency's consideration of entering into this Contract. In addition, Contractor acknowledges this is a continuing disclosure requirement. Contractor represents and warrants that Contractor shall notify System Agency in writing within five (5) business days of any changes to the representations or warranties in this clause and understands that failure to so timely update System Agency shall constitute breach of contract and may result in immediate contract termination.

31. No Felony Criminal Convictions

Contractor represents that neither Contractor nor any of its employees, agents, or representatives, including any subcontractors and employees, agents, or representative of such subcontractors, have been convicted of a felony criminal offense or that if such a conviction has occurred Contractor has fully advised System Agency in writing of the facts and circumstances surrounding the convictions.

32. Unfair Business Practices

Contractor represents and warrants that it has not been the subject of allegations of Deceptive Trade Practices violations under Chapter 17 of the Texas Business and Commerce Code, or allegations of any unfair business practice in any administrative hearing or court suit and that Contractor has not been found to be liable for such practices in such proceedings. Contractor certifies that it has no officers who have served as officers of other entities who have been the subject of allegations of Deceptive Trade Practices violations or allegations of any unfair business practices in an administrative hearing or court suit and that such officers have not been found to be liable for such practices in such proceedings**.**

33. Entities that Boycott Israel

Contractor represents and warrants that (1) it does not, and shall not for the duration of the Contract, boycott Israel or (2) the verification required by Section 2271.002 of the Texas Government Code does not apply to the Contract. If circumstances relevant to this provision change during the course of the Contract, Contractor shall promptly notify System Agency.

34. E-Verify

Contractor certifies that for contracts for services, Contractor shall utilize the U.S. Department of Homeland Security's E-Verify system during the term of this Contract to determine the eligibility of:

1. all persons employed by Contractor to perform duties within Texas; and
2. all persons, including subcontractors, assigned by Contractor to perform work pursuant to this Contract within the United States of America.

35. Former Agency Employees – Certain Contracts

If this Contract is an employment contract, a professional services contract under Chapter 2254 of the Texas Government Code, or a consulting services contract under Chapter 2254 of the Texas Government Code, in accordance with Section 2252.901 of the Texas Government Code, Contractor represents and warrants that neither Contractor nor any of Contractor's employees including, but not limited to, those authorized to provide services under the Contract, were former employees of an HHS Agency during the twelve (12) month period immediately prior to the date of the execution of the Contract.

36. Disclosure of Prior State Employment – Consulting Services

If this Contract is for consulting services,

A. In accordance with Section 2254.033 of the Texas Government Code, a Contractor providing consulting services who has been employed by, or employs an individual who has been employed by, System Agency or another State of Texas agency at any time during the two years preceding the submission of Contractor's offer to provide services must disclose the following information in its offer to provide services. Contractor hereby certifies that this information was provided and remains true, correct, and complete:

1. Name of individual(s) (Contractor or employee(s));
2. Status;
3. The nature of the previous employment with HHSC or the other State of Texas agency;
4. The date the employment was terminated and the reason for the termination; and
5. The annual rate of compensation for the employment at the time of its termination.

B. If no information was provided in response to Section A above, Contractor certifies that neither Contractor nor any individual employed by Contractor was employed by System Agency or any other State of Texas agency at any time during the two years preceding the submission of Contractor's offer to provide services.

37. Abortion Funding Limitation

Contractor understands, acknowledges, and agrees that, pursuant to Article IX of the General Appropriations Act (the Act), to the extent allowed by federal and state law, money appropriated by the Texas Legislature may not be distributed to any individual or entity that, during the period for which funds are appropriated under the Act:

1. performs an abortion procedure that is not reimbursable under the state's Medicaid program;
2. is commonly owned, managed, or controlled by an entity that performs an abortion procedure that is not reimbursable under the state's Medicaid program; or
3. is a franchise or affiliate of an entity that performs an abortion procedure that is not reimbursable under the state's Medicaid program.

The provision does not apply to a hospital licensed under Chapter 241, Health and Safety Code, or an office exempt under Section 245.004(a)(2), Health and Safety Code. Contractor represents and warrants that it is not ineligible, nor will it be ineligible during the term of this Contract, to receive appropriated funding pursuant to Article IX.

38. Funding Eligibility

Contractor understands, acknowledges, and agrees that, pursuant to Chapter 2273 of the Texas Government Code, except as exempted under that Chapter, HHSC cannot (1) contract with (a) an abortion provider or an affiliate of an abortion provider; or (b) an abortion assistance entity for the purpose of providing an abortion or abortion assistance; or (2) contract or appropriate or spend money to provide any person logistical support for

the express purpose of assisting a woman with procuring an abortion or the services of an abortion provider. Respondent certifies that it is not ineligible to contract with System Agency under the terms of Chapter 2273 of the Texas Government Code and certifies that the contract is not a taxpayer resource transaction, appropriation, or expenditure of money prohibited by Chapter 2273 of the Texas Government Code.

39. Gender Transitioning and Gender Reassignment Procedures and Treatments for Certain Children – Prohibited Use of Public Money; Prohibited State Health Plan Reimbursement.

Contractor understands, acknowledges, and agrees that, pursuant to Section 161.704 of the Texas Health and Safety Code (eff. Sept. 1, 2023), public money may not directly or indirectly be used, granted, paid, or distributed to any health care provider, medical school, hospital, physician, or any other entity, organization, or individual that provides or facilitates the provision of a procedure or treatment to a child that is prohibited under Section 161.702 of the Texas Health and Safety Code. Contractor also understands, acknowledges, and agrees that, pursuant to Section 161.705 of the Texas Health and Safety Code (eff. Sept. 1, 2023), HHSC may not provide Medicaid reimbursement and the child health plan program established under Chapter 62 may not provide reimbursement to a physician or health care provider for provision of a procedure or treatment to a child that is prohibited under Section 161.702 of the Texas Health and Safety Code. Contractor certifies that it is not ineligible to contract with System Agency under the terms of Chapter 161, Subchapter X, of the Texas Health and Safety Code.

40. Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment (2 CFR 200.216)

Contractor certifies that the individual or business entity named in this Response or Contract is not ineligible to receive the specified Contract or funding pursuant to 2 CFR 200.216.

41. COVID-19 Vaccine Passports

Pursuant to Texas Health and Safety Code, Section 161.0085(c), Contractor certifies that it does not require its customers to provide any documentation certifying the customer's COVID-19 vaccination or post-transmission recovery on entry to, to gain access to, or to receive service from the Contractor's business. Contractor acknowledges that such a vaccine or recovery requirement would make Contractor ineligible for a state-funded contract.

42. Entities that Boycott Energy Companies

In accordance with Senate Bill 13, Acts 2021, 87th Leg., R.S., pursuant to Section 2274.002 (eff. Sept. 1, 2023, Section 2276.002, pursuant to House Bill 4595, Acts 2023, 88th Leg., R.S.) of the Texas Government Code (relating to prohibition on contracts with companies boycotting certain energy companies), Contractor represents and warrants that: (1) it does not, and will not for the duration of the Contract, boycott energy companies or (2) the verification required by Section 2274.002 (eff. Sept. 1, 2023, Section 2276.002, pursuant to House Bill 4595, Acts 2023, 88th Leg., R.S.) of the Texas

Government Code does not apply to the Contract. If circumstances relevant to this provision change during the course of the Contract, Contractor shall promptly notify System Agency.

43. Entities that Discriminate Against Firearm and Ammunition Industries

In accordance with Senate Bill 19, Acts 2021, 87th Leg., R.S., pursuant to Section 2274.002 of the Texas Government Code (relating to prohibition on contracts with companies that discriminate against firearm and ammunition industries), Contractor verifies that: (1) it does not, and will not for the duration of the Contract, have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association or (2) the verification required by Section 2274.002 of the Texas Government Code does not apply to the Contract. If circumstances relevant to this provision change during the course of the Contract, Contractor shall promptly notify System Agency.

44. Security Controls for State Agency Data

In accordance with Senate Bill 475, Acts 2021, 87th Leg., R.S., pursuant to Texas Government Code, Section 2054.138, Contractor understands, acknowledges, and agrees that if, pursuant to this Contract, Contractor is or will be authorized to access, transmit, use, or store data for System Agency, Contractor is required to meet the security controls the System Agency determines are proportionate with System Agency's risk under the Contract based on the sensitivity of System Agency's data and that Contractor must periodically provide to System Agency evidence that Contractor meets the security controls required under the Contract.

45. Cloud Computing State Risk and Authorization Management Program (TX-RAMP)

In accordance with Senate Bill 475, Acts 2021, 87th Leg., R.S., pursuant to Texas Government Code, Section 2054.0593, Contractor acknowledges and agrees that, if providing cloud computing services for System Agency, Contractor must comply with the requirements of the state risk and authorization management program and that System Agency may not enter or renew a contract with Contractor to purchase cloud computing services for the agency that are subject to the state risk and authorization management program unless Contractor demonstrates compliance with program requirements. If providing cloud computing services for System Agency that are subject to the state risk and authorization management program, Contractor certifies it will maintain program compliance and certification throughout the term of the Contract.

46. Office of Inspector General Investigative Findings Expert Review

Through August 31, 2025 (when amended eff. Sep. 1, 2025, pursuant to House Bill 142, Acts 2025, 89th Leg., R.S.), if Texas Government Code, Section 544.0106 is applicable to this Contract, Contractor affirms that it possesses the necessary occupational licenses and experience.

47. Contract for Professional Services of Physicians, Optometrists, and Registered Nurses

In accordance with Senate Bill 799, Acts 2021, 87th Leg., R.S., if Texas Government Code, Section 2254.008(a)(2) is applicable to this Contract, Contractor affirms that it possesses the necessary occupational licenses and experience.

48. Foreign-Owned Companies in Connection with Critical Infrastructure

If Texas Government Code, Section 2274.0102(a)(1) (eff. Sept. 1, 2023, Section 2275.0102(a)(1), pursuant to House Bill 4595, Acts 2023, 88th Leg., R.S.) (relating to prohibition on contracts with certain foreign-owned companies in connection with critical infrastructure) is applicable to this Contract, pursuant to Government Code Section 2274.0102 (eff. Sept. 1, 2023, Section 2275.0102, pursuant to House Bill 4595, Acts 2023, 88th Leg., R.S.), Contractor certifies that neither it nor its parent company, nor any affiliate of Contractor or its parent company, is: (1) majority owned or controlled by citizens or governmental entities of China, Iran, North Korea, Russia, or any other country designated by the Governor under Government Code Section 2274.0103 (eff. Sept. 1, 2023, Section 2275.0103, pursuant to House Bill 4595, Acts 2023, 88th Leg., R.S.), or (2) headquartered in any of those countries.

49. Critical Infrastructure Subcontracts

For purposes of this Paragraph, the designated countries are China, Iran, North Korea, Russia, and any countries lawfully designated by the Governor as a threat to critical infrastructure. Pursuant to Section 117.002 of the Business and Commerce Code, Contractor shall not enter into a subcontract that will provide direct or remote access to or control of critical infrastructure, as defined by Section 117.001 of the Texas Business and Commerce Code, in this state, other than access specifically allowed for product warranty and support purposes to any subcontractor unless (i) neither the subcontractor nor its parent company, nor any affiliate of the subcontractor or its parent company, is majority owned or controlled by citizens or governmental entities of a designated country; and (ii) neither the subcontractor nor its parent company, nor any affiliate of the subcontractor or its parent company, is headquartered in a designated country. Contractor will notify the System Agency before entering into any subcontract that will provide direct or remote access to or control of critical infrastructure, as defined by Section 117.001 of the Texas Business & Commerce Code, in this state.

50. Enforcement of Certain Federal Firearms Laws Prohibited

In accordance with House Bill 957, Acts 2021, 87th Leg., R.S., if Texas Government Code, Section 2.101 is applicable to Contractor, Contractor certifies that it is not ineligible to receive state grant funds pursuant to Texas Government Code, Section 2.103.

51. Prohibition on Abortions

Contractor understands, acknowledges, and agrees that, pursuant to Article II of the General Appropriations Act, (1) no funds shall be used to pay the direct or indirect costs (including marketing, overhead, rent, phones, and utilities) of abortion procedures provided by contractors of HHSC; and (2) no funds appropriated for Medicaid Family Planning, Healthy Texas Women Program, or the Family Planning Program shall be distributed to individuals or entities that perform elective abortion procedures or that contract with or provide funds to individuals or entities for the performance of elective abortion procedures. Contractor represents and warrants that it is not ineligible, nor will it be ineligible during the term of this Contract, to receive appropriated funding pursuant to Article II.

52. Pursuant to Executive Order GA-48, relating to hardening of state government, issued November 19, 2024, Contractor certifies it is not and, if applicable, any of its holding companies or subsidiaries is not:

a. Listed in Section 889 of the 2019 National Defense Authorization Act (NDAA); or

b. Listed in Section 1260H of the 2021 NDAA; or

c. Owned by the government of a country on the U.S. Department of Commerce's foreign adversaries list under 15 C.F.R. § 791.4; or

d. Controlled by any governing or regulatory body located in a country on the U.S. Department of Commerce's foreign adversaries list under 15 C.F.R. § 791.4.

53. False Representation

Contractor understands, acknowledges, and agrees that any false representation or any failure to comply with a representation, warranty, or certification made by Contractor is subject to all civil and criminal consequences provided at law or in equity including, but not limited to, immediate termination of this Contract.

54. False Statements

Contractor represents and warrants that all statements and information prepared and submitted by Contractor in this Contract and any related Solicitation Response are current, complete, true, and accurate. Contractor acknowledges any false statement or material misrepresentation made by Contractor during the performance of this Contract or any related Solicitation is a material breach of contract and may void this Contract. Further, Contractor understands, acknowledges, and agrees that any false representation or any failure to comply with a representation, warranty, or certification made by Contractor is subject to all civil and criminal consequences provided at law or in equity including, but not limited to, immediate termination of this Contract.

55. Permits and License

Contractor represents and warrants that it will comply with all applicable laws and maintain all permits and licenses required by applicable city, county, state, and federal rules, regulations, statutes, codes, and other laws that pertain to this Contract.

56. Equal Employment Opportunity

Contractor represents and warrants its compliance with all applicable duly enacted state and federal laws governing equal employment opportunities.

57. Federal Occupational Safety and Health Law

Contractor represents and warrants that all articles and services shall meet or exceed the safety standards established and promulgated under the Federal Occupational Safety and Health Act of 1970, as amended (29 U.S.C. Chapter 15).

58. Signature Authority

Contractor represents and warrants that the individual signing this Contract Affirmations document is authorized to sign on behalf of Contractor and to bind the Contractor.

Authorized representative on behalf of Contractor must complete and sign the following:

Legal Name of Contractor
Assumed Business Name of Contractor, if applicable (d/b/a or 'doing business as')
Texas County(s) for Assumed Business Name (d/b/a or 'doing business as') **Attach Assumed Name Certificate(s) filed with the Texas Secretary of State and Assumed Name Certificate(s), if any, for each Texas County Where Assumed Name Certificate(s) has been filed.**

Signature of Authorized Representative	**Date Signed**
Printed Name of Authorized Representative **First, Middle Name or Initial, and Last Name**	**Title of Authorized Representative**
Physical Street Address	**City, State, Zip Code**
Mailing Address, if different	**City, State, Zip Code**
Phone Number	**Fax Number**
Email Address	**DUNS Number**
Federal Employer Identification Number	**Texas Identification Number (TIN)**
Texas Franchise Tax Number	**Texas Secretary of State Filing Number**
SAM.gov Unique Entity Identifier (UEI)	

Attachment F
Information Security Acceptable Use Policy

1. Purpose

This policy establishes requirements for using and protecting HHS information resources. Information resources include HHS data, information systems, and equipment.

This policy also ensures that you are informed of and agree to your responsibilities concerning the use and protection of HHS information resources.

This policy supports requirements in the Information Security Policy, Circular-021: HHS Information Security/Cybersecurity Policy, Texas Administrative Code, Chapter 202, Prohibited Technologies Security Policy, and all other relevant HHS, state, and federal policies and regulations.

2. Scope

This policy applies to all HHS desktop computers, laptops, servers, software, data, mobile devices, and any other HHS information resources that are connected to the HHS network or that process HHS data.

The scope of this policy includes equipment not owned by HHS, if it is used to access HHS data or information systems to perform HHS business.

3. Audience

This policy applies to you, if you are authorized to access HHS information resources; that is, if:

- You are an HHS workforce member, defined for the purposes of this policy as an HHS employee, intern, trainee, or volunteer.
- You are a staff augmentation contractor.
- You or your employer or contracting entity are contracted to provide services to HHS or are an external entity that has an agreement with HHS to access HHS information resources.

This policy applies when you work in a state office or in another location, such as your home.

This policy excludes members of the public who use an HHS information resource to receive services from HHS.

4. Policy

4.1 Understanding Access

Use HHS information resources only for the purposes explicitly covered in this policy, unless you are explicitly granted permission to do otherwise by the proper information owner, laws and regulations, or contract.

As an authorized user, you must only use HHS information resources for HHS business purposes or for limited personal use. Limited personal use (for example, use of email or a web browser) is explained in Chapter 1, Section D, Standards of Conduct in the HHS Human Resources Policy Manual.

Prevent and Report Unauthorized Use

Unauthorized access to or disclosure, duplication, modification, diversion, or destruction of HHS information resources is prohibited.

You must prevent unauthorized use of HHS information resources that you are authorized to use. Immediately report a suspected or known security incident or weakness to the HHS IT Customer Support Help Desk (Help Desk), per the HHS Information Security/Cybersecurity page.

Do not enter or change information in an HHS system or database without proper authorization, per Chapter 33 of the Texas Penal Code.

The Consequences of Unauthorized Use

Failure to comply with the requirements in this policy may result in disciplinary or corrective actions explained in the HHS Human Resources Policy Manual.

If you disregard the security requirements explained in this policy, such as not taking the required training or not using the HHS network appropriately, the Chief Information Security Office may:

- Notify your manager, who will take the corrective or disciplinary actions explained in Chapter 1, Section F of the HHS Human Resources Policy Manual, as appropriate.
- Require you to take training to help you understand the importance of security requirements and avoid future violations.

If you commit the following offences, you could be fined, incarcerated, or both:

- Access an HHS information resource without proper authorization.
- Give another party unauthorized access.
- Maliciously cause a computer malfunction.

4.2 Becoming an Authorized User

4.2.1. Take the Required Training

If you use HHS information resources, you must take the information security training that applies to you, even if you are not an HHS workforce member, as explained in the Information Security Training, Awareness, and Continuing Education Policy.

4.2.2. Read and Complete the Acceptable Use Agreement

Before you can access an HHS information resource for the first time, you must read this policy and complete the Acceptable Use Agreement to acknowledge that you understand and will comply with your obligations under this policy.

You may be asked to complete the Acceptable Use Agreement more than once (for example, each time you accept a new job at HHS).

You may be asked to complete the Acceptable Use Agreement in electronic format (such as on IAM Online or the Enterprise Portal), in print format, or both.

Workforce Members and Staff Augmentation Contractors

If you are a new HHS workforce member or new staff augmentation contractor, your supervisor must:

- Ensure that you complete and sign the Acceptable Use Agreement in electronic or print format during the hiring or contracting process.
- Retain a copy of your Acceptable Use Agreement.
- **Workforce members only:** Send a copy to HHS Human Resources.

Employees of Contractors and Other External Entities

If you work for an external entity and are not a staff augmentation contractor, your assigned HHS contract manager must:

- Ensure that you complete and sign the Acceptable Use Agreement electronically or in print format, when you are hired.
- Retain a copy (for example, in a contract file), if you sign the Acceptable Use Agreement outside of the HHS Enterprise Portal. (The portal retains a record.)

4.2.3. Maintain Your Authorization

After you sign the Acceptable Use Agreement, you will receive an annual reminder of your obligations under it, along with instructions to review this policy for updates. You must stay up to date on changes to the policy to retain your authorized access.

4.2.4. Have No Expectation of Privacy

When using HHS information resources, you must have no expectation of privacy, even when accessing HHS information resources from a device not owned by HHS. HHS may monitor your use of HHS information resources at any time and on any device. By using HHS information resources, you consent to being monitored.

Without notification, HHS may:

- Make subject to electronic discovery any information that you have stored in or that is associated with an HHS information resource (including personal email, voicemail, files, or messages).
- Review and provide the information for open records requests, legislative requests, litigation purposes, and investigations.

To protect your privacy and to protect against loss of personal information, avoid storing personal information on HHS information resources, particularly large files.

4.2.5. Receive Access

You will only receive access to the HHS information resources (electronic and print) that you need to perform your essential job functions, and you will be granted the least amount of access sufficient to perform those functions.

Confidential or Sensitive Information

If your essential job functions require access to information that is confidential or agency sensitive, you may be required to complete other documentation or training, in addition to reading and signing the Acceptable Use Agreement.

4.2.6. Set Up Your User Credentials

After you receive access to HHS information resources, you must set up your credentials by creating a strong password and user name, if needed.

You must use your own assigned credentials to access HHS information resources.

Never write down or store your password. If needed, use one of the approved password managers listed in the Software Catalog. Never use a Remember Password or auto logon feature, except on approved IT-managed systems.

Never reveal your password to anyone, including administrative assistants, management, or the Help Desk.

Actions initiated under your credentials are considered to be authorized and electronically signed by you.

If you suspect that your account or password is compromised, you must:

- Immediately change your password and then report it to the Help Desk.
- Follow the Help Desk's instructions to secure your account.

4.3 Accessing HHS Resources

When outside of the US or its territories, you must not access any HHS information resources owned by HHS or an HHS third-party vendor from any device using any type of network connection (wireless or physical). Such access is high risk.

4.3.1. Use Software Appropriately

You must use only HHS-approved and properly licensed software to access HHS information resources. Follow all requirements in the Software Policy and the Prohibited Technologies Security Policy.

Approved software, including mobile applications, are listed in the Software Catalog. Prohibited software is also listed, to help you know not to use it.

You must not disable or bypass malware protection software, unless you are doing so as part of your assigned job functions, and with the approval of both your manager and the HHS Chief Information Security Office.

Always follow applicable copyright laws when using HHS information resources.

4.3.2. Use the Network Appropriately

Do not modify hardware or settings to extend network capabilities. For example, you are prohibited from using or installing a device such as a wireless router on the HHS network. If you have a business need for such a device, your supervisor must submit a Help Desk ticket to get appropriate approval. This is not the same as using a home or non-HHS wireless network to connect to the HHS network with approved VPN software, which is permitted per section 4.3.4.

As explained in the Prohibited Technologies Security Policy, unless you have an approved exception per the policy:

- Do not connect to an HHS network using a device that has prohibited technology on it.
- Do not attempt to download or install a prohibited technology on a device while it's connected to an HHS network.

Confidential or Sensitive Information

To ensure that agency sensitive or confidential information, including electronic protected health information, is protected:

- Follow the guidelines in the Data Classification Standard.
- Refer to the HHS Approved Hardware List on the Requesting Hardware and Software page.

Never use chat or text messages to send confidential information.

Never circumvent security policies for internet browsing (for example, by using personal or publicly available proxy servers or devices).

4.3.3. Follow Communication Requirements

You must follow all applicable requirements for communication in Chapter 1, Section D, Standards of Conduct, in the HHS Human Resources Policy Manual.

Social Media

You must follow the guidance in Circular-042: HHS Social Media Policy and Chapter 1, Section D.14 of the HHS Human Resources Policy Manual to determine when you can use social media.

Unless you have an approved exception, you must not use social media if it is prohibited by the Prohibited Technologies Security Policy. For information on exceptions, see the policy.

Email

Do not open email attachments or links from unknown senders. Emails from senders external to HHS are identified by a banner.

Do not send unsolicited messages to large groups, except as required to conduct HHS business.

Confidential or Sensitive Information

To send confidential information by email, you must follow the requirements in 4.3.9 and in the Data Classification Standard.

Do not use your HHS email account to send confidential or agency sensitive information to your personal email account (such as a personal Gmail or Outlook account), unless it's your information (such as your tax documents or documents related to your compensation, severance, or retirement plans and benefits).

Do not use your personal email account to:

- Send HHS information that is confidential or agency sensitive.
- Receive HHS information that is confidential or agency sensitive (including from your HHS email account).
- Conduct HHS business.

Instant Messaging and Collaboration in Microsoft Teams

Use Microsoft Teams for instant messaging. Teams is HHS's standard instant messaging software.

As an authorized user, you may give another user control of a Teams meeting, but you are responsible for that user's actions, as explained in the Microsoft Teams Policy.

When using Teams, you must follow all requirements in the Microsoft Teams Policy.

4.3.4. Request Remote and VPN Access

To request VPN remote access to the HHS network, you must get your supervisor's approval, per the HHS Remote Access page.

If you are authorized to telework or to access HHS information resources from equipment not owned by HHS using remote access technology (for example, the Outlook Web access link), you must follow security practices that are equivalent to those required at your primary workplace, per the guidance on the HHS Pay, Benefits and Telework page and in 4.3.5 of this policy.

If you use HHS VPN, you must obtain your own internet service provider.

VPN automatically disconnects after a time predetermined by HHS. Maintaining an inactive connection to any technology (using Ping, StayConnect, and so on) is prohibited and may result in termination of your VPN account.

Only authorized workforce members can use remote desktop assistance to remotely access and control someone else's computer as part of their essential job functions.

4.3.5. Use Laptops, Desktops, Mobile Devices, and Printers

Unless you have an approved exception, you must follow the requirements in the Prohibited Technologies Security Policy, as they pertain to your devices:

- Do not use prohibited technology on an HHS owned or issued device.
- Do not use a personally owned device with prohibited technology on it to access HHS information resources.
- Do not use a personally owned device to record, capture, or share agency sensitive or confidential information.

For additional information, including which technologies are prohibited and how to request exceptions, see the policy.

Follow any other requirements that apply to your device, as explained below.

If you choose to use a personal device for state business, you are responsible for any associated costs.

Mobile Devices

Follow the requirements in the Using a Mobile Device to Access HHS Data Policy to appropriately use an HHS-issued or personal mobile device.

For personal mobile devices, ensure that you follow the requirements explained on the Personal Wireless Device page and comply with all HHS security policies, standards, and controls.

For information on how to request an HHS mobile device, see the State-Issued Wireless Telecommunication Equipment or Service Policy and Procedure.

Laptop and Desktop Computers

Follow the requirements in the Computing Devices and Accessories Policy to request an HHS laptop or desktop computer.

If you use a laptop or desktop computer not owned by HHS to access HHS information resources, you must use approved software to make the remote connection (such as agency-approved VPN software) or use Microsoft 365 services.

Printers

Use only HHS-owned and issued printers to print work-related documents. This includes printing from an approved telework location, such as your home.

4.3.6. Protect HHS Information

HHS information resources must be protected according to the requirements in the Data Classification Standard.

If you are aware of or suspect a security incident, a security weakness, misuse of HHS information resources, or a violation of any policy related to the security and protection of HHS information resources, you must:

- Immediately report the incident to the Help Desk.

- Follow their instructions to identify and remediate the incident.

4.3.7. Dispose of HHS-Owned Media Appropriately

You must properly dispose of (purge and destroy) digital media.

Digital media includes software, digital images and video, web pages and websites, digital data and databases, electronic documents, and digital audio such as MP3.

When using digital media, you must follow the media sanitization procedures in Information Security Controls, Media Protection (MP-01), and in the Data Classification Standard.

If you need help disposing of the media, contact the Help Desk.

Before disposing of digital media, releasing it from HHS control, or releasing it for reuse, you must sanitize it using the techniques required by the resources listed in 5.1 Federal and State Requirements.

You must dispose of physical media, such as CDs and DVDs, according to the requirements in the Data Classification Standard.

4.3.8. Maintain Physical Security and Control

Before using, disclosing, transmitting, maintaining, or creating HHS information resources (including confidential and agency sensitive information), you must obtain proper authorization and approval from your supervisor.

When removing HHS information resources (including confidential and agency sensitive information) from HHS property, you must follow the same information security policies, standards, controls, and guidelines to protect the resource, as required when using the resource at an HHS location.

To protect HHS information resources from damage, loss, or theft, you must keep them secured and under your physical control at all times and follow the safeguards explained in this policy.

Loss or Theft

If your device is lost or stolen and HHS issued it to you, or you used it to access HHS information resources, you must follow the Reporting a Lost or Stolen Device Process to file a report with the Help Desk.

4.3.9. Protect HHS Confidential Information

You must follow the Data Classification Standard when handling, processing, or managing HHS information in electronic or print format.

Encryption

Confidential and agency sensitive information must be encrypted using an HHS-approved encryption technology, per the Data Classification Standard.

Password Protection

All HHS portable or removable media (such as tablets and flash drives) containing confidential information must be password protected and encrypted with an approved FIPS 140-2 cryptographic module.

Unauthorized Viewing

When using a computer to view sensitive or confidential information, you must position it to prevent unauthorized viewing or access.

Key Cards

Immediately upon becoming aware that a keycard is lost or stolen, report it to the appropriate facility manager.

Do not:

- Leave keys used to access confidential or sensitive information unattended.
- Distribute, copy, loan, or share a keycard or other access mechanism, unless doing so is part of your specific job functions.

When you no longer need a keycard or other access mechanism, you must return it to the office or area that issued it.

IRS Federal Tax Information

If you suspect any of the following, file an incident report immediately (before 24 hours has elapsed) with the HHS IRS coordinator:

- An unauthorized person has accessed federal tax information (FTI).
- An authorized person has disclosed FTI to an unauthorized person or accessed FTI without a need to know (that is, without a business reason).

- An authorized person has printed FTI, or downloaded, copied, or saved FTI to another location. These actions make FTI more susceptible to unauthorized access.

If the reported action is an incident, the IRS coordinator notifies HHS Privacy. Privacy investigates by taking the steps explained in Circular-057: Protecting Confidential Information and Responding to Privacy Breaches and the Privacy Incident Response Plan, notifies the appropriate contacts, and responds to the incident according to the requirements in IRS Publication 1075.

In some cases, an incident may be both a privacy and an information security incident. In such cases, the Information Security Incident Response Policy, Information Security Incident Response Process, and Information Security Incident Response Plan also apply.

Loss or Theft

As a proactive measure, you must be prepared, at a minimum, to describe the agency sensitive or confidential information on a device that you are in possession of, in case the device is lost or stolen.

If the device is lost or stolen, you must follow the Reporting a Lost or Stolen Device Process to file a report with the Help Desk. When making your report, describe the agency sensitive or confidential information on the device.

Also report the loss or theft of agency sensitive or confidential information to:

- Your supervisor or manager.
- The chief information security officer, and other agency or HHS offices as applicable, as explained in the Information Security Incident Response Policy.
- The HHS Privacy Division's Incident Response team, per the instructions on the HHS Privacy Division's page and in Circular-057: Protecting Confidential Information and Responding to Privacy Breaches.

5. Related Resources

Some resources are restricted to people with access rights.

5.1 Federal and State Requirements

Federal Information Processing Standard (FIPS) 140-2

Specifies the security requirements that must be satisfied by a cryptographic module.

Texas Administrative Code, Chapter 202, Information Security Standards

Establishes the information security standards followed by state agencies in Texas.

Texas Penal Code, Title 7, Chapter 33, Computer Crimes

Defines Texas law related to securing computers and data.

IRS Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies

Explains the security guidelines for protecting federal tax returns and tax return information.

5.2 Policies and Standards

HHS Human Resources Policy Manual

Establishes requirements for employment, benefits, leave, and compensation.

Circular-021: HHS Information Security/Cybersecurity Policy

Explains how HHS protects HHS information resources.

Information Security Policy

Provides a framework for the protection of HHS information resources.

Data Classification Standard

Communicates the required protections for HHS information resources.

Information Security Controls

Explains the safeguards and countermeasures needed to satisfy information security requirements.

Circular-042: HHS Social Media Policy

Establishes clear standards and responsibilities for the use of social media tools to increase awareness of state programs and services according to state law, codes, and HHS policies and procedures.

Software Policy

Establishes requirements for software used within the HHS system, including requirements related to requesting, licensing, installing, removing, auditing, and tracking software.

Information Security Incident Response Policy

Establishes requirements for reporting, prioritizing, and handling information security incidents involving HHS information resources.

Information Security Training, Awareness, and Continuing Education Policy

Establishes information security training, awareness, and continuing education requirements to protect HHS.

Microsoft Teams Policy

Establishes requirements for the use of Microsoft Teams for the HHS system.

Circular-057: Protecting Confidential Information and Responding to Privacy Breaches

Establishes the HHS policies for safeguarding confidential information and reporting and responding to privacy breaches.

Using a Mobile Device to Access HHS Data Policy

Establishes HHS acceptable use, maintenance, and security requirements for mobile devices that are used to access HHS data.

Computing Devices and Accessories Policy

Establishes requirements for HHS issued laptop and desktop computers and their accessories, such as how to request or return them.

Prohibited Technologies Security Policy

Establishes the technologies that are prohibited by the Governor of Texas or DIR and the measures HHS is required to take to prevent their use.

State-Issued Wireless Telecommunication Equipment or Service Policy and Procedure

Establishes eligibility and other requirements for state-issued mobile phones.

5.3 Processes and Procedures

Information Security Incident Response Process

Establishes the requirements for reporting, prioritizing, and handling information security incidents that involve HHS information resources.

Reporting a Lost or Stolen Device Process

Explains how to report a device as lost or stolen if it can be used to access HHS information and what actions are taken when a report is made.

5.4 Definitions and Other

HHS Acceptable Use Agreement

Informs authorized users of their responsibilities when using HHS information resources.

HHSC Software Catalog

Catalog of software approved for use by authorized users.

Information Security Incident Response Plan

Confidential internal procedures used to respond to security incidents.

Privacy Incident Response Plan

Confidential internal procedures used to respond to privacy incidents.

IT Glossary

Provides definitions for technical or specialized terms.

6. Revision History

Published	Effective	Change Type	Change Summary	Owner
04/28/2023	04/28/2023	Revised	Read change summary	Chief Information Security Office
02/15/2023	02/15/2023	Revised	Read change summary	Chief Information Security Office
06/23/2022	06/23/2022	Revised	Read change summary	Chief Information Security Office
8/13/2021	8/13/2021	Revised	Read change summary	Chief Information Security Office
7/15/2015	7/15/2015	Issued	N/A	Chief Information Security Office

Request Revisions

For revisions to this document, submit a request form.

Information Security Acceptable Use Agreement

You must complete this agreement if you use HHS information resources.

Before signing this agreement, read the Information Security Acceptable Use Policy in its entirety and make sure that you understand it. If you need help accessing the policy, speak to your supervisor or contract manager.

Acknowledgement

I have read, understand, and will comply with the requirements in the Information Security Acceptable Use Policy.

Your Signature (required):

Your Name Printed (required):

Your Work Email (required):

Your Work Phone (required):

I am (required: choose one and explain below):

- ☐ An employee of HHSC (specify department and division):
- ☐ An employee of DSHS (specify department and division):
- ☐ An employee of another agency (specify agency, department, and division):
- ☐ A contractor (specify employer or non-state agency name):
- ☐ An intern or volunteer (specify agency, department, and division):
- ☐ Other (specify, for example, if you are an advisory council member or an employee of a private provider):

HHS Employee ID, if applicable:

Date Agreement Signed (required):