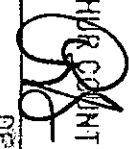


DEPARTMENT OF STATE HEALTH SERVICES



2018 APR 30 AM 10:17
UPSHUR COUNTY, TX.
BY  DEPUTY
COUNTY CLERK

FILED
TERRY ROSS
COUNTY CLERK

Contract number HHSREV100000915 (the "Contract"), is entered into by Department of State Health Services ("DSHS") Vital Statistics Section and Upshur County ("Contractor"). DSHS and Contractor are collectively referred to herein as the "Parties."

- I. **Purpose of the Contract.** DSHS agrees to provide access to the DSHS Vital Event Electronic Registration System for the purpose of issuing individual birth certificates.
- II. **Term of the Contract.** This Contract will begin on September 1, 2018 and end on August 31, 2023.
- III. **Authority.** The Parties enter into this Contract under the authority of Texas Health and Safety Code Chapter 191 and Texas Government Code Chapter 791.
- IV. **Statement of Work.**
 - A. DSHS agrees to provide on-line computer services in support of Contractor from 7:00 a.m. to 6:00 p.m. (CST) Monday through Friday, except holidays. In the event of an emergency or computer application error, DSHS may temporarily suspend services without advance notice.
 - B. Contractor may search DSHS databases, locate data, and issue Certifications of Birth to authorized individuals requesting such data. The certifications will be in a format formally approved by DSHS. Contractor will take reasonable efforts to ensure use of the DSHS Vital Event Electronic Registration System is not abused by its staff. Abuse of the access to confidential information in the DSHS Vital Event Electronic Registration System may be cause for termination of this Contract in accordance with Section IX.K.
 - C. Contractor will acquire the necessary data processing equipment, communications, hardware or software, and purchase "bank note" paper, as specified by DSHS. DSHS will assist in connection of the equipment, furnish software program and provide technical assistance, if necessary.
 - D. Contractor will complete the DSHS Vital Event Electronic Registration System registration forms as specified by DSHS. Contractor will remain in compliance with any requirements specified by DSHS for accessing the DSHS Vital Event Electronic Registration System. Contractor will not be required to pay an additional fee pursuant to this Subsection.
 - E. Contractor acknowledges that records may not be located in the searching process instituted by Contractor, or records which are located may have errors due to:

1. Normal key-entry errors in spellings;
 2. Accidental failure on the part of the DSHS to update a file for an amendment or paternity determination; and
 3. The event year does not exist on the system.
- F. Contractor will notify DSHS in writing, at least monthly of errors or suspected errors that exist on the database information.
- G. Contractor is to maintain an inventory control and account for each document produced on "bank note" paper, including voided documents.
- H. Contractor will issue Certificates of Birth utilizing remote access to the DSHS system in conformance with Health and Safety Code Chapters 191, 192 and 195, as well as 25 Tex. Admin. Code Chapter 181.
- I. The Parties are required to comply with all applicable state and federal laws relating to the privacy and confidentiality of this data and records, which includes Texas Government Code Section 552.115.
- J. The Parties will use confidential records and information obtained under this Contract only for purposes as described in this Contract and as otherwise allowed by law.

V. Fees.

Contractor agrees to pay DSHS ONE DOLLAR AND EIGHTY-THREE CENTS (\$1.83) for each Certification of Vital Record printed as a result of searches of the database. Contractor agrees to charge the same base search fee for a birth certificate as DSHS. Additional fees may only be charged as authorized by Texas Health and Safety Code Chapter 191 and 25 Tex. Admin. Code Chapter 181.

VI. Billing.

- A. DSHS will send an itemized billing to Contractor on a monthly basis for each Certification of Birth printed. This billing will be sent through the U.S. Postal Service to the Contractor at:

Name: Upshur County Clerk's Office
Address: P.O. Box 730
Gilmer, TX 75644

- B. Contractor will direct any billing inquiries either by phone to 512-776-7206 or email to vsubusinessservices@dshs.texas.gov.

VII. Payment Method.

- A. Contractor will remit payment to DSHS within thirty days after a billing is received by them. Payment by the Contractor will be considered made on the date postmarked.

- B. Contractor will send payments to DSHS at:

Texas Department of State Health Services
Cash Receipts Branch MC 2096
P.O. Box 149347
Austin, TX 78714-9347

- C. Contractor will make payment to DSHS out of its current revenues.

VIII. Representatives. The following will act as the Representative authorized to administer activities under this Contract on behalf of their respective Party.

Upshur County	DSHS
Upshur County Upshur County Clerk's Office Attn: Terri Ross P.O. Box 730 Gilmer, TX 75644 Phone: (903) 843-4015 Email: terri.ross@countyofupshur.com	Texas Department of State Health Services Contract Management Section Attn: Carolyn DeBoer Mail Code 1990 P.O. Box 149347 Austin, TX 78714-9347 Phone: (512) 776-2265 Email: Carolyn.deboer@dshs.texas.gov

IX. General Terms and Conditions.

- A. **Governing Law.** Regarding all issues related to this Contract's formation, performance, interpretation, and any issues that may arise in any dispute between the parties, the Contract will be governed by and construed in accordance with the laws of the State of Texas.

- B. **Amendment.** This Contract may be modified by written amendment signed by the Parties.

- C. **Confidentiality.**
The Parties are required to comply with all applicable state and federal laws relating to the privacy and confidentiality of records that contain Personal Identifying Information (PII) or Personally Sensitive Information (PSI) or other information or records made confidential by law, including Tex. Bus. & Comm. Code Section 521.002. The attached Data Use Agreement (Attachment A) applies to this Contract.

- D. Exchange of Personal Identifying Information.** This Contract concerns personal identifying information. Except as prohibited by other law, Contractor and DSHS may exchange PII without consent, in accordance with Chapter 191 of the Health and Safety Code.
- E. Records Retention.** DSHS will retain records in accordance with DSHS State of Texas Records Retention Schedule at <http://www.dshs.texas.gov/records/schedules.shtm>, Department Rules and other applicable state and federal statutes and regulations governing medical, mental health, and substance abuse information.
- F. Severability.** If any provision of this Contract is construed to be illegal or invalid, the illegal or invalid provision will be deemed stricken and deleted to the same extent and effect as if never incorporated, but all other provisions will continue.
- G. Notice.** Any notice required or permitted to be given under this Contract will be in writing and sent to the respective Party's Representative in Section VIII. Notice will be deemed to have been received by a Party on the third business day after the date on which it was mailed to the Party at the address specified in writing by the Party to the other Party, or, if sent by certified mail, on the date of receipt.
- H. Waiver.** Acceptance by either Party of partial performance or failure to complain of any action, non-action or default under this Contract will not constitute a waiver of either Party's rights under the Contract.
- I. Assignment.** Neither DSHS nor Contractor will transfer, assign, or sell its interest, in whole or in part, in this Contract without prior written consent by both Parties.
- J. Suspension of Services Under This Contract.** In the event of an emergency or information technology system failure, DSHS may temporarily suspend services without advance notice. Use of services for purposes inconsistent with applicable law may also result in a suspension of services.
- K. Termination.**
- 1. Convenience.** This Contract may be terminated by mutual agreement of the Parties. Either Party may terminate this Contract without cause by giving 30 days written notice of its intent to terminate to the non-terminating Party.
 - 2. Cause.** This Contract may be terminated for cause by either Party for breach or failure to perform an essential requirement of the Contract. Use of services for purposes inconsistent with applicable law may be cause for Contract termination.
 - 3. Notice of Termination.** Written notice may be sent by any method that provides verification of receipt, which will be calculated from the date of receipt by the non-terminating Party's Representative provided in Section VIII.

Contract Number: HHSREV100000915

4: Equitable Settlement. At the end of the Term of this Contract or termination as provided for in this Section, the Parties will equitably settle their respective accrued interests or obligations incurred prior to termination.

By signing below, the Parties agree that this Contract constitutes the entire legal and binding agreement between them. The Parties acknowledge that they have read the Contract and agree to its terms, and that the persons whose signatures appear below have the authority to execute this Contract on behalf of their respective Party.

DEPARTMENT OF STATE HEALTH SERVICES

UPSHUR COUNTY

Manda Hall MD

Dean Fowler

Manda Hall, M.D.
Associate Commissioner
Department of State Health Services

Dean Fowler
County Judge
Upshur County

4/18/18
Date *MH*

4/30/18
Date

THE FOLLOWING ATTACHMENTS ARE ATTACHED AND INCORPORATED AS PART OF THE CONTRACT HHSREV100000915:

ATTACHMENT A- DATA USE AGREEMENT

FILED
UPSHUR
COUNTY CLERK
APR 30 2018
UPSHUR COUNTY, TX.
BY *[Signature]*
DEPUTY

ATTACHMENT A – DATA USE AGREEMENT

DATA USE AGREEMENT BETWEEN THE TEXAS HEALTH AND HUMAN SERVICES ENTERPRISE AND UPSHUR COUNTY (“CONTRACTOR”)

This Data Use Agreement (“DUA”) is incorporated into System Agency Contract No. HHSREV100000915 (the “Base Contract”) between the Texas Department of State Health Services (“System Agency”) and Upshur County (“Contractor”).

ARTICLE 1. PURPOSE; APPLICABILITY; ORDER OF PRECEDENCE

ATTACHMENT 1. 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 and the limited purposes for which the Contractor may create, receive, maintain, use, disclose or have access to Confidential Information. 45 CFR 164.504(e)(1)-(3). This DUA also describes System Agency’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 System Agency, its programs or clients as described in the Base Contract.

As of the Effective Date of the Contract, 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 Scope of Work of the Base Contract for Contractor to fulfill its obligations under the Base Contract, or any other purpose expressly authorized by System Agency 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 create, receive, maintain, use, disclose or have access to on behalf of System Agency 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.

“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; Estates Code Ch. 752 and Texas Prob. Code § 3.

ARTICLE 3. CONTRACTOR'S DUTIES REGARDING CONFIDENTIAL INFORMATION

Section 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) Contractor will not, without System Agency's prior written consent, 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 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 the Authorized Purpose or as Required by Law.

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

(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 System Agency 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, without prior written approval of System Agency, disclose or provide access to any Confidential Information on the basis that such act is Required by Law without notifying System Agency so that System Agency may have the opportunity to object to the disclosure or access and seek appropriate relief. If System Agency objects to such disclosure or access, Contractor will refrain from disclosing or providing access to the Confidential Information until System Agency has exhausted all alternatives for relief. *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 System Agency 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, on behalf of Contractor without requiring that Subcontractor first execute the Form Subcontractor Agreement, Attachment 1, which ensures that the Subcontractor will comply with the identical terms, conditions, safeguards and restrictions as contained in this DUA for PHI and any other relevant Confidential Information and which permits more strict limitations; and *45 CFR 164.502(e)(1)(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, Contractor will make PHI available to System Agency in a Designated Record Set or, as directed by System Agency, provide PHI to the Individual, or Legally Authorized Representative of the Individual who is requesting PHI in compliance with the requirements of the HIPAA Privacy Regulations. 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. *45 CFR 164.524 and 164.504(e)(2)(ii)(E)*

(I) Contractor will make PHI as required by HIPAA available to System Agency for amendment and incorporate any amendments to this information that System Agency directs or agrees to pursuant to the HIPAA. *45 CFR 164.504(e)(2)(ii)(E) and (F)*

(J) Contractor will document and make available to System Agency 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 by any Individual subject to this DUA, it will promptly forward the request to System Agency; however, if it would violate HIPAA to forward the request, Contractor will promptly notify of the request and of Contractor's response. Unless Contractor is prohibited by law from forwarding a request, System Agency will respond to all such requests, unless System Agency has given prior written consent for Contractor to respond to and account for all such requests. *45 CFR 164.504(e)(2)*

(L) Contractor will provide, and will cause its Subcontractors and agents to provide, to System Agency 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 or disclose PHI for the proper management and administration of Contractor or to carry out Contractor's legal responsibilities if: 45 CFR 164.504(e)(ii)(I)(A)

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

(2) Contractor obtains reasonable assurances from the Person to whom the information is disclosed that the Person 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 requested by System Agency, use PHI to provide data aggregation services to System Agency, 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, return to System Agency or Destroy, at System Agency's election, and to the extent reasonably feasible and permissible by law, all Confidential Information received from System Agency or created or maintained by Contractor or any of Contractor's agents or Subcontractors on System Agency's behalf if that data contains Confidential Information. Contractor will certify in writing to System Agency that all the Confidential Information that has been created, received, maintained, used by or disclosed to Contractor, has been Destroyed or returned to System Agency, and that Contractor and its agents and Subcontractors have retained no copies thereof. Notwithstanding the foregoing, Contractor acknowledges and agrees that it may not Destroy any Confidential Information if federal or state law, or System Agency record retention policy or a litigation hold notice prohibits such Destruction. If such return or Destruction is not reasonably feasible, or is impermissible by law, Contractor will immediately notify System Agency of the reasons such return 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 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, or maintains Confidential Information, Contractor will complete and return to System Agency at infosecurity@hhsc.state.tx.us the System Agency information security and privacy initial inquiry (SPI) at Attachment 2. The SPI identifies basic privacy and security controls with which Contractor must comply to protect System Agency Confidential Information. Contractor will comply with periodic security controls compliance assessment and monitoring by System Agency 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 System Agency

Confidential Information and will provide the updated document to System Agency. System Agency 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 any and all appropriate 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, subject to System Agency approval, 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 System Agency upon execution of this DUA and prior to any change. *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 System Agency, 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 DUA. *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 on behalf of System Agency for System Agency's review and approval within 30 days of execution of this DUA and upon request by System Agency the following business day or other agreed upon time frame. *45 CFR 164.308; 164.514(d)*

(X) Contractor will make available to System Agency any information System Agency requires to fulfill System Agency'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, or other federal or state law. *45 CFR 164.504(e)(2)(i)(1)*

(Y) Contractor will only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form. A secure transmission of electronic Confidential Information in motion includes secure File Transfer Protocol (SFTP) or Encryption at an appropriate level or otherwise protected as required by rule, regulation or law. System Agency Confidential Information at rest requires Encryption unless there is adequate administrative, technical, and physical security, or as otherwise

protected as required by rule, regulation or law. All electronic data transfer and communications of Confidential Information will be through secure systems. Proof of system, media or device security or Encryption must be produced to System Agency no later than 48 hours after System Agency'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 System Agency 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) Contractor will comply with the following laws and standards *if applicable to the type of Confidential Information and Contractor's Authorized Purpose*:

- 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 System Agency program area that Contractor supports on behalf of System Agency.

ARTICLE 4. BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS

Section 4.01. Breach or Event Notification to System Agency. 45 CFR 164.400-414

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

(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 System Agency's satisfaction (the "incident response period"). *45 CFR 164.404*

(C) Breach Notice:

1. Initial Notice.

System Agency Data Use Agreement V.8.3 HIPAA Omnibus Compliant April 1, 2015

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 System Agency in writing, initially report to System Agency's Privacy and Security Officers via email at: privacy@SystemAgencyC.state.tx.us and to the System Agency 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 System AgencyC-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 System Agency for, Contractor's single point of contact who will communicate with System Agency both on and off business' hours during the incident response period.

2. 48-Hour Formal Notice. No later than 48 consecutive clock hours after Discovery, or a time within which Discovery reasonably should have been made by Contractor of an Event or Breach of Confidential Information, provide formal notification to the State, 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 System Agency 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 System Agency's approval as to the steps Individuals 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 of 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 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 System Agency, 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 System Agency requests following Discovery.

Section 4.02 Investigation, Response and Mitigation. For A-F below: 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 System Agency for incident response purposes and for purposes of System Agency's compliance with report and notification requirements, to the satisfaction of System Agency.

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

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

(D) Contractor will fully cooperate with System Agency'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 System Agency in a Corrective Action Plan if directed by System Agency under the Base Contract.

Section 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) System Agency may direct Contractor to provide Breach notification to Individuals, regulators or third-parties, as specified by System Agency following a Breach.

(B) Contractor must obtain System Agency's prior written approval of the time, manner and content of any notification to Individuals, regulators or third-parties, or any notice required by other state or federal authorities. Notice letters will be in Contractor's name and on Contractor's letterhead, unless otherwise directed by System Agency, and will contain contact information, including the name and title of Contractor's representative, an email address and a toll-free telephone number, for the Individual to obtain additional information.

(C) Contractor will provide System Agency with copies of distributed and approved communications.

(D) Contractor will have the burden of demonstrating to the satisfaction of System Agency that any notification required by System Agency 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 System Agency delegates notice requirements to Contractor, System Agency 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. SCOPE OF WORK

Scope 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 System Agency that are described in detail in the Base Contract. The Scope 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

Section 6.01 *Ownership of Confidential Information*

Contractor acknowledges and agrees that the Confidential Information is and will remain the property of System Agency. Contractor agrees it acquires no title or rights to the Confidential Information.

Section 6.02 *System Agency Commitment and Obligations*

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

Section 6.03 *System Agency Right to Inspection*

At any time upon reasonable notice to Contractor, or if System Agency determines that Contractor has violated this DUA, System Agency, 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, System Agency's agent(s) include, without limitation, the System Agency Office of the Inspector General or the Office of the Attorney General of Texas, outside consultants or legal counsel or other designee.

Section 6.04 *Term; Termination of DUA; Survival*

This DUA will take effect with the Base Contract, and will terminate upon termination of the Base Contract and as set forth herein. If the Base Contract is extended or amended, this DUA is updated automatically concurrent with such extension or amendment.

(A) System Agency 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 System Agency.

(D) If System Agency determines that Contractor has violated a material term of this DUA; System Agency may in its sole discretion:

1. Exercise any of its rights including but not limited to reports, access and inspection under this DUA 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 System Agency may determine necessary to maintain compliance with this DUA; or

3. Provide Contractor with a reasonable period to cure the violation as determined by System Agency; or

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

Before exercising any of these options, System Agency will provide written notice to Contractor describing the violation and the action it intends to take.

(E) If neither termination nor cure is feasible, System Agency shall report the violation to the Secretary.

(F) 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 System Agency, as required by this DUA.

Section 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 Travis County, 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.

Section 6.06 *Injunctive Relief*

(A) Contractor acknowledges and agrees that System Agency 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 System Agency for Contractor's or its Subcontractor's failure to comply. Accordingly, Contractor agrees that System Agency 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.

Section 6.07 *Indemnification*

To the extent permitted by law, Contractor will indemnify, defend and hold harmless System Agency and its respective Executive Commissioner, employees, Subcontractors, agents (including other state agencies acting on behalf of System Agency) or other members of its Workforce (each of the foregoing hereinafter referred to as "Indemnified Party") against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this DUA or from any acts or omissions related to this DUA by Contractor or its employees, directors, officers, Subcontractors, or agents or other members of its Workforce. The duty to indemnify, defend and hold harmless is independent of the duty to insure and continues to apply even in the event insurance coverage required, if any, in the DUA or Base Contract is denied, or coverage rights are reserved by any insurance carrier. Upon demand, Contractor will reimburse System Agency for any and all losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party to the extent caused by and which results from the Contractor's failure to meet any of its obligations under this DUA. To the extent permitted

by law, Contractor's obligation to defend, indemnify and hold harmless any Indemnified Party will survive the expiration or termination of this DUA.

Section 6.08 Insurance

(A) Contractor represents and warrants that it maintains either self-insurance or commercial insurance with policy limits sufficient to cover any liability arising from any acts or omissions by Contractor or its employees, directors, officers, Subcontractors, or agents or other members of its Workforce under this DUA. Contractor warrants that System Agency will be a loss payee and beneficiary for any such claims.

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

Section 6.09 Fees and Costs

Except as otherwise specified in this DUA or the Base Contract, including but not limited to requirements to insure or indemnify System Agency, 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.

Section 6.10 Entirety of the Contract

This Data Use Agreement is incorporated by reference into the Base Contract 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.

Section 6.11 Automatic Amendment and Interpretation

Upon the effective date of any amendment or issuance of additional regulations to HIPAA, or any other law applicable to Confidential Information, this DUA will automatically be amended so that the obligations imposed on System Agency or Contractor remain in compliance with such requirements. Any ambiguity in this DUA will be resolved in favor of a meaning that permits System Agency and Contractor to comply with HIPAA or any other law applicable to Confidential Information.

ATTACHMENT 1. SUBCONTRACTOR AGREEMENT FORM

System Agency CONTRACT NUMBER HHSREV100000915

The DUA between System Agency and Contractor establishes the permitted and required uses and disclosures of Confidential Information by Contractor.

Contractor has subcontracted with _____ (SUBContractor) for performance of duties on behalf of CONTACTOR which are subject to the DUA. SUBContractor acknowledges, understands and agrees to be bound by the identical terms and conditions applicable to Contractor under the DUA, incorporated by reference in this Agreement, with respect to System Agency Confidential Information. Contractor and SUBContractor agree that System Agency is a third-party beneficiary to applicable provisions of the subcontract.

System Agency has the right but not the obligation to review or approve the terms and conditions of the subcontract by virtue of this Subcontractor Agreement Form.

Contractor and SUBContractor assure System Agency that any Breach or Event as defined by the DUA that SUBContractor Discovers will be reported to System Agency by Contractor in the time, manner and content required by the DUA.

If Contractor knows or should have known in the exercise of reasonable diligence of a pattern of activity or practice by SUBContractor that constitutes a material breach or violation of the DUA or the SUBContractor's obligations Contractor will:

1. Take reasonable steps to cure the violation or end the violation, as applicable;
2. If the steps are unsuccessful, terminate the contract or arrangement with SUBContractor, if feasible;
3. Notify System Agency immediately upon reasonably discovery of the pattern of activity or practice of SUBContractor that constitutes a material breach or violation of the DUA and keep System Agency reasonably and regularly informed about steps Contractor is taking to cure or end the violation or terminate SUBCONTRACTOR's contract or arrangement.

This Subcontractor Agreement Form is executed by the parties in their capacities indicated below.

CONTRACTOR

SUBCONTRACTOR

BY: _____

BY: _____

NAME: _____

NAME: _____

TITLE: _____

TITLE: _____

DATE _____, 201 .

DATE: _____



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 in sections B and C prior to the contract award date. If you are an applicant for an open enrollment, you must have corrected any "No" answers in Sections B and C below prior to performing any work on behalf of any HHS agency. For existing contracts or renewals with "No" responses, there must be an action plan for remediation of Section B and C within 30 calendar days for HIPAA related contracts and 90 calendar days from the date the form is signed for all non-HIPAA contracts.

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

<p>1. Does the applicant/bidder access, create, disclose, receive, transmit, maintain, or store 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.</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p>2. Entity or Applicant/Bidder Legal Name</p>	<p>Legal Name: Legal Entity Tax Identification Number (TIN) (Last Four Numbers Only): Procurement/Contract#: Address: City: State: ZIP: Telephone #: Email Address:</p>
<p>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.</p>	<p>Total Employees:</p>
<p>4. Number of Subcontractors (if Applicant/Bidder will not use subcontractors, enter "0")</p>	<p>Total Subcontractors:</p>
<p>5. Name of Information Technology Security Official and Name of Privacy Official for Applicant/Bidder (Privacy and Security Official may be the same person.)</p>	<p>A. Security Official: Legal Name: Address: City: State: ZIP: Telephone #: Email Address:</p> <p>B. Privacy Official: Legal Name: Address: City: State: ZIP: Telephone #: Email Address:</p>

6. Type(s) of HHS Confidential Information the Entity or Applicant/Bidder will create, receive, maintain, use, disclose or have access to: (Check all that apply) <ul style="list-style-type: none"> • 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 <input type="checkbox"/>	CJIS <input type="checkbox"/>	IRS FTI <input type="checkbox"/>	CMS <input type="checkbox"/>	SSA <input type="checkbox"/>	PII <input type="checkbox"/>
Other (Please List) 						
7. Number of Storage Devices for HHS Confidential Information (as defined in the HHS 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) 0					
a. Devices. Number of personal user computers, devices or drives, including mobile devices and mobile drives.						
b. Servers. Number of Servers that are not in a data center or using Cloud Services.						
c. Cloud Services. Number of Cloud Services in use.						
d. Data Centers. Number of Data Centers in use.						
8. Number of unduplicated individuals for whom Applicant/Bidder reasonably expects to handle HHS Confidential Information during one year:	Select Option					
a. 499 individuals or less b. 500 to 999 individuals c. 1,000 to 99,999 individuals d. 100,000 individuals or more	<input type="radio"/> a. <input type="radio"/> b. <input type="radio"/> c. <input type="radio"/> d.					
9. HIPAA Business Associate Agreement	Yes or No					
a. Will Applicant/Bidder use, disclose, create, receive, transmit or maintain protected health information on behalf of a HIPAA-covered HHS agency for a HIPAA-covered function?	<input type="radio"/> Yes <input type="radio"/> 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 "No" if not applicable, such as for agencies not covered by HIPAA.)	<input type="radio"/> Yes <input type="radio"/> No					
10. Subcontractors. If the Applicant/Bidder responded "0" to Question 4 (indicating no subcontractors), check "No" for both 'a.' and 'b.' to indicate "N/A."	Yes or No					
a. Does Applicant/Bidder require subcontractors to execute the DUA Attachment 1 Subcontractor Agreement Form?	<input type="radio"/> Yes <input type="radio"/> No					
b. Will Applicant/Bidder obtain written approval from an HHS agency before entering into any agreements with subcontractors to handle HHS Confidential Information on behalf of Applicant/Bidder?	<input type="radio"/> Yes <input type="radio"/> No					

<p>11. Does Applicant/Bidder have any Optional Insurance currently in place?</p> <p>Optional Insurance provides coverage for: (1) Network Security and Privacy; (2) Data Breach; (3) Cyber Liability (lost data, lost use or delay/suspension in business, denial of service with e-business, the Internet, networks and informational assets, such as privacy, intellectual property, virus transmission, extortion, sabotage or web activities); (4) Electronic Media Liability; (5) Crime/Theft; (6) Advertising Injury and Personal Injury Liability; and (7) Crisis Management and Notification Expense Coverage.</p>	<input type="radio"/> Yes <input type="radio"/> No
--	---

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 items is 30 calendar days, PII related items is 90 calendar days.

1. Written Policies & Procedures. Does Applicant/Bidder have current written privacy and security policies and procedures that, at a minimum:

<p>a. Does Applicant/Bidder have current written privacy and security policies and procedures that identify Authorized Users and Authorized Purposes (as defined in the DUA) relating to creation, receipt, maintenance, use, disclosure, access or transmission of HHS Confidential Information?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>b. 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 HHS Confidential Information on behalf of an HHS agency?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>c. Does Applicant/Bidder have current written privacy and security policies and procedures that limit use or disclosure of HHS Confidential Information to the minimum that is necessary to fulfill the Authorized Purposes?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>d. Does Applicant/Bidder have current written privacy and security policies and procedures that respond to an actual or suspected breach of HHS Confidential Information, to include at a minimum (if any responses are "No" check "No" for all three):</p> <ul style="list-style-type: none"> i. Immediate breach notification to the 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 HHS Confidential Information has been breached, as directed by the HHS agency? 	<input type="radio"/> Yes <input type="radio"/> No

<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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 HHS Confidential Information, to carry out an obligation under the DUA for an Authorized Purpose, unless otherwise approved in writing by an HHS agency?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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 HHS Confidential Information in violation of the DUA, the Base Contract or applicable law?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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 HHS Confidential Information within 60 days of identification of a need for update?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

<p>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 HHS Confidential Information, or attempt to contact any Individuals whose records are contained in the HHS Confidential Information, except for an Authorized Purpose, without express written authorization from an HHS agency or as expressly permitted by the Base Contract?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>k. If Applicant/Bidder intends to use, disclose, create, maintain, store or transmit HHS Confidential Information outside of the United States of America, will Applicant/Bidder obtain the express prior written permission from the HHS agency and comply with the HHS agency conditions for safeguarding offshore HHS Confidential Information?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>l. Does Applicant/Bidder have current written privacy and security policies and procedures that require cooperation with HHS agencies' or federal regulatory inspections, audits or investigations related to compliance with the DUA or applicable law?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>m. Does Applicant/Bidder have current written privacy and security policies and procedures that require appropriate standards and methods to destroy or dispose of HHS Confidential Information?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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 HHS pursuant to the DUA, or to publish HHS Confidential Information without express prior approval of the HHS agency?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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 HHS Confidential Information. Training must include: (1) privacy and security policies, procedures, plans and applicable requirements for handling HHS Confidential Information, (2) a requirement to complete training before access is given to HHS Confidential Information, and (3) written proof of training and a procedure for monitoring timely completion of training.</p>	<input type="radio"/> Yes <input type="radio"/> No

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

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

This section is about your electronic system. If your business DOES NOT store, access, or transmit 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 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 compliant 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 HHS agency

- Yes
 No

For more information regarding FIPS 140-2 encryption products, please refer to:
<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

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 HHS Confidential Information (e.g., a formal process exists for granting access and validating the need for users to access 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 HHS Confidential Information.

- Yes
 No

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


Action Plan for Compliance with a Timeline:

Compliance Date:

<p>5. Does each member of Applicant/Bidder's Workforce who will use, disclose, create, receive, transmit or maintain HHS Confidential Information have a unique user name (account) and private password?</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>6. Does Applicant/Bidder lock the password after a certain number of failed attempts and after 15 minutes of user inactivity in all computing devices that access or store HHS Confidential Information?</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>7. Does Applicant/Bidder secure, manage and encrypt remote access (including wireless access) to computer systems containing HHS Confidential Information? (e.g., a formal process exists for granting access and validating the need for users to remotely access HHS Confidential Information, and remote access is limited to Authorized Users).</p> <p><i>Encryption is required for all HHS Confidential Information. Additionally, FIPS 140-2 compliant 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.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm</i></p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>8. Does Applicant/Bidder implement computer security configurations or settings for all computers and systems that access or store HHS Confidential Information? (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit exploitation opportunities for hackers or intruders, etc.)</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>9. Does Applicant/Bidder secure physical access to computer, paper, or other systems containing HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.)?</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>

<p>10. Does Applicant/Bidder use encryption products to protect HHS Confidential Information that is <u>transmitted</u> over a public network (e.g., the Internet, WiFi, etc.).</p> <p>If yes, upon request must provide evidence such as a screen shot or a system report.</p> <p><i>Encryption is required for all HHS Confidential Information. Additionally, FIPS 140-2 compliant 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.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm</i></p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>11. Does Applicant/Bidder use encryption products to protect HHS Confidential Information <u>stored</u> on end user devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.)?</p> <p>If yes, upon request must provide evidence such as a screen shot or a system report.</p> <p><i>Encryption is required for all HHS Confidential Information. Additionally, FIPS 140-2 compliant 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.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm</i></p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>12. Does Applicant/Bidder require Workforce members to formally acknowledge rules outlining their responsibilities for protecting HHS Confidential Information and associated systems containing HHS Confidential Information before their access is provided?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>13. Is Applicant/Bidder willing to perform or submit to a criminal background check on Authorized Users?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>14. Does Applicant/Bidder prohibit the access, creation, disclosure, reception, transmission, maintenance, and storage of HHS Confidential Information with a subcontractor (e.g. cloud services, social media, etc.) unless HHS has approved the subcontractor agreement which must include compliance and liability clauses with the same requirements as the Applicant/Bidder?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>

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 HHS Confidential Information?	<input type="radio"/> Yes <input type="radio"/> No	
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>	
16. Do Applicant/Bidder's computing systems that use, disclose, access, create, transmit, maintain or store HHS Confidential Information contain up-to-date anti-malware and antivirus protection?	<input type="radio"/> Yes <input type="radio"/> No	
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>	
17. Does the Applicant/Bidder review system security logs on computing systems that access or store HHS Confidential Information for abnormal activity or security concerns on a regular basis?	<input type="radio"/> Yes <input type="radio"/> No	
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>	
18. Notwithstanding records retention requirements, does Applicant/Bidder's disposal processes for HHS Confidential Information ensure that HHS Confidential Information is destroyed so that it is unreadable or undecipherable?	<input type="radio"/> Yes <input type="radio"/> No	
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>	
Section D: Signature and Submission		
<i>Please sign the form digitally, if possible. If you can't, provide a handwritten signature.</i>		
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 HHS of this immediately.		
2. Signature	3. Title	4. Date:
To submit the completed, signed form: <ul style="list-style-type: none"> Email the form as an attachment to the appropriate HHS Contract Manager. 		

Section E: To Be Completed by HHS Agency Staff:		
Agency(s): HHSC: <input type="checkbox"/> DADS: <input type="checkbox"/> DFPS: <input type="checkbox"/> DSHS: <input type="checkbox"/>		Requesting Department(s):
Legal Entity Tax Identification Number (TIN) (Last four Only):  <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>		PO/Contract(s) #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:

INSTRUCTIONS FOR COMPLETING THE SECURITY AND PRIVACY INITIAL INQUIRY (SPI)

Attachment 2 to the HHS Enterprise Data Use Agreement

Below are instructions for Applicants, Bidders and Contractors for 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 in sections B and C prior to the contract award date. If you are an applicant for an open enrollment, you must have corrected any "No" answers in Sections B and C below prior to performing any work on behalf of any HHS agency. For existing contracts or renewals with "No" responses, there must be an action plan for remediation of Section B and C within 30 calendar days for HIPAA related contracts and 90 days for others from the date the form is signed

SECTION A. APPLICANT /BIDDER INFORMATION

Item #1. *Only contractors that access, transmit, store, and/or maintain Confidential Information will complete and email this form as an attachment to the appropriate 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 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 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 HHS Confidential Information that the Contractor will create, receive, maintain, use, disclose or have access to. The DUA section Article 2, Definitions, defines 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 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 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 HHS Confidential Information.
- **Item 7b. Servers.** Provide the number of servers not housed in a data center or "in the cloud," on which 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 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 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 Applicant/Bidder reasonably expects to handle 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 Service, 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."
- **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 "no."

Item #10. Subcontractors. If your business responded "0" to question 3 (number of subcontractors), Answer "no" to Items 9a and 9b 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 HHS approval before permitting subcontractors to handle 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 do not have this optional coverage, answer "no."

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 HHS Confidential Information and respond in the event of a Breach of 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.

For any question Section B or Section C question that is answered "no", an explanation of how compliance will be corrected and a date when compliance will be complete in the designated areas below the question.

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 HHS Confidential Information. The policies and procedures should also identify the reason why these Authorized Users need to access the 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 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 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 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, 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 a suspected breach of 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 HHS, the 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 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 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 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 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 HHS Confidential Information to only persons who have been authorized and trained on how to handle 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 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 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 HHS Confidential Information except to perform obligations under the contract, or with written permission from HHS.
- **Item #1k.** Answer "yes" if your business has written policies and procedures prohibiting you from using, disclosing, creating, maintaining, storing or transmitting 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 HHS Confidential Information. Policies and procedures should comply with 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 HHS pursuant to the DUA, or other 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 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 HHS Confidential Information. If you are the only person with access to 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 HHS Confidential Information. If you are the only one with access to 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 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 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 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 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 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 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:

<http://windows.microsoft.com/en-us/windows/change-password-policy-settings#1TC=windows-7>

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 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 HHS Confidential Information. If your business uses a Microsoft Windows system, refer to the Microsoft website on how to do this, see example:

<http://windows.microsoft.com/en-us/windows/change-password-policy-settings#1TC=windows-7>

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 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 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:

<http://windows.microsoft.com/en-us/windows7/Security-checklist-for-Windows-7>

Item #9. Answer "yes" if your business secures physical access to computer, paper, or other systems containing 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 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 compliant 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/groups/STM/cmvp/documents/140-1/140val-all.htm>).

Item #11. Answer "yes" if your business stores 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 compliant encryption products, please refer to: <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>). If you do not utilize end-

user electronic devices for storing 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 HHS Confidential Information and associated systems containing 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 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 HHS Confidential Information on Cloud Services or social media sites if you use such services or sites, and there is an 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 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 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:

<http://windows.microsoft.com/en-US/windows7/products/features/windows-update>

Item #16. Answer "yes" if your business's computing systems that use, disclose, access, create, transmit, maintain or store 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:

<http://windows.microsoft.com/en-US/windows7/products/features/windows-update>


Item #17. Answer "yes" if your business reviews system security logs on computing systems that access or store 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:

<http://windows.microsoft.com/en-us/windows/what-information-event-logs-event-viewer#1TC=windows-7>

Item #18. Answer "yes" if your business disposal processes for HHS Confidential Information ensures that 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.

SECTION D. SIGNATURE AND SUBMISSION

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

FILED
TERRI ROSS
CLERK
2018 APR 30 AM 10:17
UPSHUR COUNTY, TX.
BY  DEPUTY