TEXAS Health and Human Services

HHS Enterprise Data Use Agreement - Attachment 2
SECURITY AND PRIVACY INITIAL INQUIRY (SPI)

If you are a bidder for a new procurement/contract, in order to participate in the bidding process, you must have corrected any "No" responses 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)

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.**	(●) Yes ( ) No
2. Entity or Applicant/Bidder Legal Name	Legal Name: Fort Bend County Legal Entity Tax Identification Number (TIN) (Last Four Numbers Only): 1969 Procurement/Contract#: HHSREV100000828 Address: 301 Jackson Street City: Richmond State: TX ZIP: 77469 Telephone #: (281) 341-8685 Email Address: cclerk@fortbendcountytx.gov
3. Number of Employees, at all locations, in Applicant Bidder's Workforce "Workforce" means all employees, volunteers, trainees, and other Persons whose conduct is under the direct control of Applicant/Bidder, whether or not they are paid by Applicant/ Bidder. If Applicant/Bidder is a sole proprietor, the workforce may be only one employee.	Total Employees: 25
4. Number of Subcontractors (if Applicant/Bidder will not use subcontractors, enter "0")	Total Subcontractors: 0
5. Name of Information Technology Security Official and Name of Privacy Official for Applicant/Bidder (Privacy and Security Official may be the same person.)	**A. Security Official:** Legal Name: Ray Webb Address: 301 Jackson Street City: Richmond State: TX ZIP: 77469 Telephone #: (281) 341-4570 Email Address: Ray.Webb@fortbendcountytx.gov
	B. Privacy Official: Legal Name: Ray Webb Address: 301 Jackson Street City: Richmond State: TX ZIP: 77469 Telephone #: (281) 341-4570 Email Address: Ray.Webb@fortbendcountytx.gov

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) • *Health Insurance Portability and Accountability Act (HIPAA) data* • *Criminal Justice Information Services (CJIS) data* • *Internal Revenue Service Federal Tax Information (IRS FTI) data* • *Centers for Medicare & Medicaid Services (CMS)* • *Social Security Administration (SSA)* • *Personally Identifiable Information (PII)*	HIPAA ☐	CJIS ☐	IRS FTI ☐	CMS ☐	SSA ☐	PII ☑
	Other (Please List)					

7. Number of Storage Devices for 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) 20
a. Devices. Number of personal user computers, devices or drives, including mobile devices and mobile drives.	18
b. Servers. Number of Servers that are not in a data center or using Cloud Services.	2
c. Cloud Services. Number of Cloud Services in use.	0
d. Data Centers. Number of Data Centers in use.	0
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	◉ a. ○ b. ○ c. ○ 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?	○ Yes ◉ No
b. Does Applicant/Bidder have a Privacy Notice prominently displayed on a Webpage or a Public Office of Applicant/Bidder's business open to or that serves the public? (This is a HIPAA requirement. Answer "No" if not applicable, such as for agencies not covered by HIPAA.)	○ Yes ◉ 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?	○ Yes ◉ 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?	○ Yes ◉ No

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

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:	**Yes or No**
a. Does Applicant/Bidder have current written privacy and security policies and procedures that identify Authorized Users and Authorized Purposes (as defined in the DUA) relating to creation, receipt, maintenance, use, disclosure, access or transmission of HHS Confidential Information?	○ Yes ◉ No
Action Plan for Compliance with a Timeline: Commit to create policy & procedure no later than 90 days from execution date	Compliance Date:
b. Does Applicant/Bidder have current written privacy and security policies and procedures that require Applicant/Bidder and its Workforce to comply with the applicable provisions of HIPAA and other laws referenced in the DUA, relating to creation, receipt, maintenance, use, disclosure, access or transmission of HHS Confidential Information on behalf of an HHS agency?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
c. Does Applicant/Bidder have current written privacy and security policies and procedures that limit use or disclosure of HHS Confidential Information to the minimum that is necessary to fulfill the Authorized Purposes?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
d. Does Applicant/Bidder have current written privacy and security policies and procedures that respond to an actual or suspected breach of HHS Confidential Information, to include at a minimum (if any responses are "No" check "No" for all three): 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?	◉ Yes ○ No

Action Plan for Compliance with a Timeline:	Compliance Date:
e. Does Applicant/Bidder have current written privacy and security policies and procedures that conduct annual workforce training and monitoring for and correction of any training delinquencies?	○ Yes ◉ No
Action Plan for Compliance with a Timeline: Commit to create policy & procedure no later than 90 days from execution date	Compliance Date:
f. Does Applicant/Bidder have current written privacy and security policies and procedures that permit or deny individual rights of access, and amendment or correction, when appropriate?	○ Yes ◉ No
Action Plan for Compliance with a Timeline: Commit to create policy & procedure no later than 90 days from execution date	Compliance Date:
g. Does Applicant/Bidder have current written privacy and security policies and procedures that permit only Authorized Users with up-to-date privacy and security training, and with a reasonable and demonstrable need to use, disclose, create, receive, maintain, access or transmit the HHS Confidential Information, to carry out an obligation under the DUA for an Authorized Purpose, unless otherwise approved in writing by an HHS agency?	○ Yes ◉ No
Action Plan for Compliance with a Timeline: Commit to create policy & procedure no later than 90 days from execution date	Compliance Date:
h. Does Applicant/Bidder have current written privacy and security policies and procedures that establish, implement and maintain proof of appropriate sanctions against any Workforce or Subcontractors who fail to comply with an Authorized Purpose or who is not an Authorized User, and used or disclosed HHS Confidential Information in violation of the DUA, the Base Contract or applicable law?	○ Yes ◉ No
Action Plan for Compliance with a Timeline: Commit to create policy & procedure no later than 90 days from execution date	Compliance Date:
i. Does Applicant/Bidder have current written privacy and security policies and procedures that require updates to policies, procedures and plans following major changes with use or disclosure of HHS Confidential Information within 60 days of identification of a need for update?	○ Yes ◉ No
Action Plan for Compliance with a Timeline: Commit to create policy & procedure no later than 90 days from execution date	Compliance Date:

j. Does Applicant/Bidder have current written privacy and security policies and procedures that restrict permissions or attempts to re-identify or further identify de-identified 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?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
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?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
l. Does Applicant/Bidder have current written privacy and security policies and procedures that require cooperation with HHS agencies' or federal regulatory inspections, audits or investigations related to compliance with the DUA or applicable law?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
m. Does Applicant/Bidder have current written privacy and security policies and procedures that require appropriate standards and methods to destroy or dispose of HHS Confidential Information?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
n. Does Applicant/Bidder have current written privacy and security policies and procedures that prohibit disclosure of Applicant/Bidder's work product done on behalf of HHS pursuant to the DUA, or to publish HHS Confidential Information without express prior approval of the HHS agency?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
2. Does Applicant/Bidder have a current Workforce training program? Training of Workforce must occur at least once every year, and within 30 days of date of hiring a new Workforce member who will handle 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.	○ Yes ◉ No

Action Plan for Compliance with a Timeline: Commit to create policy & procedure no later than 90 days from execution date	Compliance Date:
3. Does Applicant/Bidder have Privacy Safeguards to protect HHS Confidential Information in oral, paper and/or electronic form? "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.	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
4. Does Applicant/Bidder and all subcontractors (if applicable) maintain a current list of Authorized Users who have access to HHS Confidential Information, whether oral, written or electronic?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
5. Does Applicant/Bidder and all subcontractors (if applicable) monitor for and remove terminated employees or those no longer authorized to handle HHS Confidential Information from the list of Authorized Users?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

Section C: SECURITY RISK ANALYSIS AND ASSESSMENT (to be completed by Applicant/Bidder)	
This section is about your electronic system. If your business DOES NOT store, access, or transmit 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 *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*	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
2. Does Applicant/Bidder utilize an IT security-knowledgeable person or company to maintain or oversee the configurations of Applicant/Bidder's computing systems and devices?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
3. Does Applicant/Bidder monitor and manage access to 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. **If yes, upon request must provide evidence such as a screen shot or a system report.**	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

5. Does each member of Applicant/Bidder's Workforce who will use, disclose, create, receive, transmit or maintain HHS Confidential Information have a unique user name (account) and private password?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
6. Does Applicant/Bidder lock the password after a certain number of failed attempts and after 15 minutes of user inactivity in all computing devices that access or store HHS Confidential Information?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
7. Does Applicant/Bidder secure, manage and encrypt remote access (including wireless access) to computer systems containing 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). *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.* *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*	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
8. Does Applicant/Bidder implement computer security configurations or settings for all computers and systems that access or store HHS Confidential Information? (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit exploitation opportunities for hackers or intruders, etc.)	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
9. Does Applicant/Bidder secure physical access to computer, paper, or other systems containing HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.)?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

10. Does Applicant/Bidder use encryption products to protect HHS Confidential Information that is *transmitted* over a public network (e.g., the Internet, WiFi, etc.). **If yes, upon request must provide evidence such as a screen shot or a system report.** *Encryption is required for all HHS Confidential Information. Additionally, **FIPS 140-2** 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*	○ Yes ◉ No
Action Plan for Compliance with a Timeline: No accessible to the public	Compliance Date:
11. Does Applicant/Bidder use encryption products to protect HHS Confidential Information *stored* on end user devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.)? **If yes, upon request must provide evidence such as a screen shot or a system report.** *Encryption is required for all 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.* *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*	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
12. Does Applicant/Bidder require Workforce members to formally acknowledge rules outlining their responsibilities for protecting HHS Confidential Information and associated systems containing HHS Confidential Information before their access is provided?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
13. Is Applicant/Bidder willing to perform or submit to a criminal background check on Authorized Users?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
14. Does Applicant/Bidder prohibit the access, creation, disclosure, reception, transmission, maintenance, and storage of 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?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

15. Does Applicant/Bidder keep current on security updates/patches (including firmware, software and applications) for computing systems that use, disclose, access, create, transmit, maintain or store HHS Confidential Information?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
16. Do Applicant/Bidder's computing systems that use, disclose, access, create, transmit, maintain or store HHS Confidential Information contain up-to-date anti-malware and antivirus protection?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
17. Does the Applicant/Bidder review system security logs on computing systems that access or store HHS Confidential Information for abnormal activity or security concerns on a regular basis?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
18. Notwithstanding records retention requirements, does Applicant/Bidder's disposal processes for HHS Confidential Information ensure that HHS Confidential Information is destroyed so that it is unreadable or undecipherable?	◉ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

Section D: Signature and Submission

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

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

2. Signature	3. Title	4. Date:
[signature]	Fort Bend County Clerk	8/30/18

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

- Email the form as an attachment to the appropriate HHS Contract Manager.

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