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: Williamson County<br>Legal Entity Tax Identification Number (TIN) (Last Four Numbers Only): 978<br>Procurement/Contract#: not applicable<br>Address: 405 Martin Luther King St., Ste. 203<br>City: Georgetown State: TX ZIP: 78626<br>Telephone #: (512) 943-1515<br>Email Address: nrister@wilco.org |
| **3.** **Number of Employees, at all locations, in Applicant Bidder's Workforce**<br>"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: 43 |
| **4.** **Number of Subcontractors**<br>(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**<br>(Privacy and Security Official may be the same person.) | **A. Security Official:**<br>Legal Name: Paul Hulse<br>Address: 301 SW Inner Loop, Ste. 105<br>City: Georgetown State: TX ZIP: 78626<br>Telephone #: (512) 943-1456<br>Email Address: phulse@wilco.org |
| | **B. Privacy Official:**<br>Legal Name: Nancy Rister<br>Address: 405 Martin Luther King St., Ste. 203<br>City: Georgetown State: TX ZIP: 78626<br>Telephone #: (512) 943-1515<br>Email Address: nrister@wilco.org |

| **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)**<br>• *Health Insurance Portability and Accountability Act (HIPAA) data*<br>• *Criminal Justice Information Services (CJIS) data*<br>• *Internal Revenue Service Federal Tax Information (IRS FTI) data*<br>• *Centers for Medicare & Medicaid Services (CMS)*<br>• *Social Security Administration (SSA)*<br>• *Personally Identifiable Information (PII)* | HIPAA ☐ | CJIS ☐ | IRS FTI ☐ | CMS ☐ | SSA ☐ | PII ☑ |
|---|---|---|---|---|---|---|
| | Other (Please List)<br>Local Registrar-NOT A STATE AGENCY | | | | | |

| **7.Number of Storage Devices for HHS Confidential Information (as defined in the HHS Data Use Agreement (DUA))**<br>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.<br><br>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)<br>1 |
|---|---|
| **a. Devices.** Number of personal user computers, devices or drives, including mobile devices and mobile drives. | 1 |
| **b. Servers.** Number of Servers that are not in a data center or using Cloud Services. | 0 |
| **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<br>**b.** 500 to 999 individuals<br>**c.** 1,000 to 99,999 individuals<br>**d.** 100,000 individuals or more | ◉ a.<br>○ b.<br>○ c.<br>○ 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<br>◉ 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<br>◉ 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<br>◉ 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<br>◉ No |

| | |
|---|---|
| **11.** Does Applicant/Bidder have any **Optional Insurance** currently in place?<br>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<br>○ 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<br>○ No |
| Action Plan for Compliance with a Timeline: | Compliance Date: |
| **b.** Does Applicant/Bidder have current written privacy and security policies and procedures that require Applicant/Bidder and its Workforce to comply with the applicable provisions of HIPAA and other laws referenced in the DUA, relating to creation, receipt, maintenance, use, disclosure, access or transmission of HHS Confidential Information on behalf of an HHS agency? | ◉ Yes<br>○ 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<br>○ 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):<br>i. Immediate breach notification to the HHS agency, regulatory authorities, and other required Individuals or Authorities, in accordance with Article 4 of the DUA;<br>ii. Following a documented breach response plan, in accordance with the DUA and applicable law; &<br>iii. Notifying Individuals and Reporting Authorities whose HHS Confidential Information has been breached, as directed by the HHS agency? | ◉ Yes<br>○ 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<br>○ No |
| Action Plan for Compliance with a Timeline: | Compliance Date: |
| **f.** Does Applicant/Bidder have current written privacy and security policies and procedures that permit or deny individual rights of access, and amendment or correction, when appropriate? | ◉ Yes<br>○ No |
| Action Plan for Compliance with a Timeline: | Compliance Date: |
| **g.** Does Applicant/Bidder have current written privacy and security policies and procedures that permit only Authorized Users with up-to-date privacy and security training, and with a reasonable and demonstrable need to use, disclose, create, receive, maintain, access or transmit the 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<br>○ No |
| Action Plan for Compliance with a Timeline: | Compliance Date: |
| **h.** Does Applicant/Bidder have current written privacy and security policies and procedures that establish, implement and maintain proof of appropriate sanctions against any Workforce or Subcontractors who fail to comply with an Authorized Purpose or who is not an Authorized User, and used or disclosed HHS Confidential Information in violation of the DUA, the Base Contract or applicable law? | ◉ Yes<br>○ No |
| Action Plan for Compliance with a Timeline: | Compliance Date: |
| **i.** Does Applicant/Bidder have current written privacy and security policies and procedures that require updates to policies, procedures and plans following major changes with use or disclosure of HHS Confidential Information within 60 days of identification of a need for update? | ◉ Yes<br>○ No |
| Action Plan for Compliance with a Timeline: | Compliance Date: |

| | |
|---|---|
| **j.** Does Applicant/Bidder have current written privacy and security policies and procedures that restrict permissions or attempts to re-identify or further identify de-identified 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<br>○ 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<br>○ 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<br>○ 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<br>○ 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<br>○ No |
| Action Plan for Compliance with a Timeline: | Compliance Date: |
| **2.** Does Applicant/Bidder have a current Workforce training program?<br>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<br>○ No |

| | |
|---|---|
| Action Plan for Compliance with a Timeline: | Compliance Date: |
| **3.** Does Applicant/Bidder have Privacy Safeguards to protect HHS Confidential Information in oral, paper and/or electronic form?<br>"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<br>( ) 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<br>( ) 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<br>( ) 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?<br>**a.** The data is encrypted with FIPS 140-2 compliant encryption<br>**b.** The offshore provider does not have access to the encryption keys<br>**c.** The Applicant/Bidder maintains the encryption key within the United States<br>**d.** The Application/Bidder has obtained the express prior written permission of the HHS agency<br>*For more information regarding FIPS 140-2 encryption products, please refer to:*<br>*http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm* | ◉ Yes<br>○ 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<br>○ 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<br>○ 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.<br>**If yes, upon request must provide evidence such as a screen shot or a system report.** | ◉ Yes<br>○ 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:<br>Not applicable - the system is controlled by DSHS. | 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).<br><br>*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.*<br><br>*For more information regarding FIPS 140-2 encryption products, please refer to:*<br>*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.).<br><br>**If yes, upon request must provide evidence such as a screen shot or a system report.**<br>*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.*<br><br>*For more information regarding FIPS 140-2 encryption products, please refer to:*<br>*http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm* | ○ Yes<br>○ No |
| Action Plan for Compliance with a Timeline:<br>Not applicable. | 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.)?<br>**If yes, upon request must provide evidence such as a screen shot or a system report.**<br>*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.*<br><br>*For more information regarding FIPS 140-2 encryption products, please refer to:*<br>*http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm* | ○ Yes<br>○ No |
| Action Plan for Compliance with a Timeline:<br>Not applicable. | 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<br>○ 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<br>○ 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<br>○ No |
| Action Plan for Compliance with a Timeline:<br>Not applicable. | 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<br>○ 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<br>○ 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<br>○ No |
| Action Plan for Compliance with a Timeline:<br>Not applicable. | 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<br>○ 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: |
|---|---|---|
| | | |

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):<br>HHSC: ☐ DADS: ☐ DFPS: ☐ DSHS: ☐ | Requesting Department(s): | |
| Legal Entity Tax Identification Number (TIN) (Last four Only):<br>■ ■ ■ ■ ■ ■ ■ | 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 H H S 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.