DEPARTMENT OF STATE HEALTH SERVICES

This Memorandum of Understanding (MOU) is entered into between the Department of State Health Services (DSHS) and Fort Bend County by and through Fort Bend County Health & Human Services ("Contractor") who are collectively referred to herein as the "Parties."

I. **Purpose of the MOU**. DSHS agrees to provide Contractor certain confidential data extracted from designated death records which DSHS maintains. The Parties agree to the intended utilization of the data as outlined in Attachment B of this MOU. No personally identifiable or non-public data will be shared or released by Contractor, without specific statutory authority.

II. **Term of the MOU**. Unless terminated as provided for in Section V (C), this MOU will become effective on the signature date of the latter of the Parties to sign this MOU, and end on December 31, 2025. The Parties may renew this MOU for one additional five-year term by executing a written amendment. Data will not be shared among Parties without a written agreement in place. If the agreement expires then data sharing will cease.

III. **Authority**. The Parties enter into this MOU under the authority of:

a) Texas Health and Safety Code, Title 12, Section 1001.089.
b) Texas Health and Safety Code, Title 3, Section 193.011.
c) Texas Health and Safety Code, Title 2.
d) Texas Government Code, Chapter 791, Interlocal Cooperation Act.

IV. **Statement of Work.**

A. DSHS will deliver to Contractor dynamic death data files via secure website data exchange, according to the variables approved by DSHS Attachment B (Confidential Data), which are attached and incorporated as part of this MOU. In dynamic death files, variables which will be provided include only those items in Attachment B that are available for dynamic data.

B. Data sent will be regarding all deaths related to or associated with COVID-19 for the duration of the outbreak or until termination of this MOU, whichever occurs first. The data to be shared is outlined in Attachment B. The selection criteria are deaths among all residents of the Contractor's jurisdiction. Contractor may request changes or additional variables by submitting the request through the Assigned Contract Manager for review and approval in writing.

C. Files containing the Confidential Data will be delivered to Contractor, as available.

D. This death data is being supplied to support Contractor's response to the COVID-19 pandemic. Confidential Data shall not be used for any other purposes unless specifically approved in writing by DSHS and in compliance with Contractor's appropriate review. DSHS will provide its approval or denial in writing.

E. The method of delivery of Confidential Data will be through the use of a secure file transfer protocol (SFTP) site or other method of data transfer with at least that same level of security and/or encryption whose internet address, log-in and password identification will be sent by DSHS personnel to Contractor's Representative (as noted in Section VI).

V. General Terms and Conditions.

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

B. **Confidentiality**.

1. The Parties are required to comply with all applicable state and federal laws relating to the privacy and confidentiality of Confidential Data and records.
2. Contractor will comply with the Data Use Agreement incorporated into this MOU as Attachment A.
3. Contractor will maintain sufficient safeguards to prevent release or disclosure of any such confidential records or information obtained under this MOU to anyone other than individuals who are authorized by law to receive such records or information and who will protect the records or information from re-disclosure as required by law. Data will be housed in a secure location. The foregoing shall not apply to information that:
   (i) is not disclosed in writing by DSHS or reduced to writing and marked confidential within thirty (30) days after disclosure; or
   (ii) is already in Contractor possession at the time of disclosure as evidenced by written records in the possession of Contractor prior to such time; or
   (iii) is or later becomes part of the public domain through no fault of Contractor; or
   (iv) is received from a third party having no obligations of confidentiality to DSHS; or
   (v) is independently developed by Contractor or by its personnel having no access to the Confidential Data.
4. Contractor will use Confidential Data obtained under this MOU only for purposes as described in this MOU and as otherwise allowed by law.
5. Notwithstanding any provision relating to confidentiality, the confidential information held by DSHS may be disclosed to a third party pursuant to the Texas Public Information Act (Texas Government Code Chapter 552), any open records decision or ruling by the Attorney General that such information constitutes public information, or as otherwise provided by law.
6. Any remaining Confidential Data provided as part of this MOU will be destroyed within 60-days of the termination of the MOU.
7. Data no longer in use will be destroyed using software that renders these data unrecoverable.

C. Termination.
Either Party may terminate this MOU without cause by giving thirty (30) days' written notice of its intent to terminate to the non-terminating Party.

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

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

F. Right to Audit
The Parties acknowledge the State Auditor's authority to conduct audits of state agencies under Chapter 321 of the Texas Government Code.

G. Assignment
No assignment of this MOU or of any right accruing hereunder shall be made, in whole or part, by either Party without the prior written consent of the other, unless authorized by law.

H. Dispute Resolution
The Parties agree to use good faith efforts to resolve all questions, difficulties, or disputes of any nature that may arise under or by this MOU; provided however, nothing in this paragraph shall preclude either Party from pursuing any remedies available under Texas law.

I. Force Majeure
Neither Party shall be liable to the other for any delay in, or failure of performance of, any requirement included in this MOU caused by force majeure. The existence of such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been removed provided the non-performing Party exercises all reasonable due diligence to perform. Force majeure is defined as acts of God, war, fires, explosions, hurricanes, floods, failure of transportation, or other causes that are beyond the reasonable control of either Party and that by exercise of due foresight such Party could not reasonably have been expected to avoid, and which, by the exercise of all reasonable due diligence, such Party is unable to overcome.

J. No Waiver
This MOU shall not constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies, or immunities available to either Party as an agency of the State of Texas or otherwise available to the Party. The failure to enforce or any delay in the enforcement of any privileges, rights, defenses, remedies, or immunities available to a Party under this MOU or under applicable law shall not constitute a waiver of such privileges, rights, defenses, remedies, or immunities or be considered as a basis for estoppel. Neither Party waives any privileges, rights, defenses, or immunities available to it as an agency of the State of Texas, or otherwise available to it, by entering into this MOU or by its conduct prior to or subsequent to entering into this MOU.

K. **Governing Law and Venue**

The Parties agree that this MOU in all respects shall be governed by and constructed in accordance with the laws of the state of Texas, except for its provisions regarding conflicts of laws. The venue of any suit sought in connection with terms and conditions of this agreement is fixed in any court of competent jurisdiction in Travis County, Texas, unless mandated otherwise by statute.

VI. **Authorized Representatives**. The following will act as the Representative authorized to administer activities under this MOU on behalf of their respective Party.

Contract Management Section (CMS)	Regional Local Health Operations	Contractor
Stacie Flenoy Contract Manager 1100 W 49th Street, MC1990 Austin, Texas 78756 Telephone: (512) 776-2265 Email: stacie.fenoy@dshs.texas.gov	Glenna Laughlin, Regional & Local Coord. Team Lead 1100 W 49th Street Austin, Texas 78756 Telephone: (512) 776-6323 Email: glenna.laughlin@dshs.texas.gov	Jacquelyn Johnson-Minter Director of Health and Human Services 94520 Reading Road, Ste. A Rosenberg, Texas 77471 Telephone: (281) 238-3233 Email: Jacquelyn.Minter@fortbendcountytx.gov

VII. **Legal Notices**

Legal Notices under this MOU shall be deemed delivered when deposited either in the United States mail, postage paid, certified, return receipt requested; or with a common carrier, overnight, signature required, to the appropriate address below:

DSHS
Department of State Health Services
Attn: General Counsel
100 W. 49th Street, MC1911
Austin, Texas 78756

Contractor
Fort Bend County Department of Health and Human Services
94520 Reading Road, Ste. A
Rosenberg, Texas 77471

Notice given in any other manner shall be deemed effective only if and when received by the Party to be notified. Either Party may change its address for receiving legal notice by notifying the other Party in writing.

VIII. CERTIFICATIONS

The undersigned contracting Parties certify that:

(1) the services specified herein are necessary and essential for activities that are properly within the statutory functions and programs of the affected agencies of state government;

(2) Each Party executing this MOU on its behalf has full power and authority to enter into this MOU;

(3) the proposed arrangements serve the interest of efficient and economical administration of state government; and

(4) the services contracted for are not required by Section 21, Article XVI of the Constitution of Texas to be supplied under a contract awarded to the lowest responsible bidder.

DSHS further certifies that it has statutory authority to contract for the services described in this contract under Texas Health and Safety Code, Title 2.

Contractor further certifies that it has statutory authority to contract for the services described in this contract under the authority outlined in Section III.

SIGNATURE PAGE FOLLOWS

SIGNATURE PAGE

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

Texas Department of State Health Services

David Gruber
Associate Commissioner

Date of Execution: 9/22/2020

Contractor

Date of Execution: 9.8.2020

THE FOLLOWING ATTACHMENTS TO ARE HEREBY ATTACHED AND INCORPORATEDBY REFERENCE:

ATTACHMENT A	**DATA USE AGREEMENT (DUA)**
ATTACHMENT A-1	**SECURITY AND PRIVACY INQUIRY (SPI)**
ATTACHMENT B	**CHECKLIST FOR DEATH DATA COVID**
ATTACHMENT C	**LIST OF INDIVIDUALS ACCESSING VITAL DATA**

Attachment A

HHS DATA USE AGREEMENT

This Data Use Agreement ("DUA"), effective as of the date the Base Contract into which it is incorporated is signed ("Effective Date"), is entered into by and between a Texas Health and Human Services Enterprise agency ("HHS"), and the Contractor identified in the Base Contract, a political subdivision of the State of Texas ("CONTRACTOR.

ARTICLE 1.
PURPOSE; APPLICABILITY; ORDER OF PRECEDENCE

The purpose of this DUA is to facilitate creation, receipt, maintenance, use, disclosure or access to Confidential Information with CONTRACTOR, and describe CONTRACTOR's rights and obligations with respect to the Confidential Information. ***45 CFR 164.504(e)(1)-(3)***. This DUA also describes HHS's remedies in the event of CONTRACTOR's noncompliance with its obligations under this DUA. This DUA applies to both Business Associates and contractors who are not Business Associates who create, receive, maintain, use, disclose or have access to Confidential Information on behalf of HHS, its programs or clients as described in the Base Contract.

As of the Effective Date of this DUA, if any provision of the Base Contract, including any General Provisions or Uniform Terms and Conditions, conflicts with this DUA, this DUA controls.

ARTICLE 2.
DEFINITIONS

For the purposes of this DUA, capitalized, underlined terms have the meanings set forth in the following: Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (42 U.S.C. §1320d, *et seq.*) and regulations thereunder in 45 CFR Parts 160 and 164, including all amendments, regulations and guidance issued thereafter; The Social Security Act, including Section 1137 (42 U.S.C. §§ 1320b-7), Title XVI of the Act; The Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a and regulations and guidance thereunder; Internal Revenue Code, Title 26 of the United States Code and regulations and publications adopted under that code, including IRS Publication 1075; OMB Memorandum 07-18; Texas Business and Commerce Code Ch. 521; Texas Government Code, Ch. 552, and Texas Government Code §2054.1125. In addition, the following terms in this DUA are defined as follows:

"Authorized Purpose" means the specific purpose or purposes described in the Statement of Work of the Base Contract for CONTRACTOR to fulfill its obligations under the Base Contract, or any other purpose expressly authorized by HHS in writing in advance.

"Authorized User" means a Person:

(1) Who is authorized to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze Confidential Information pursuant to this DUA;

(2) For whom CONTRACTOR warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to the Confidential Information; and

(3) Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information as required by this DUA.

"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to CONTRACTOR, or that CONTRACTOR may, for an Authorized Purpose, create, receive, maintain, use, disclose or have access to, that consists of or includes any or all of the following:

(1) Client Information;

(2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information (herein "PHI");

(3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;

(4) Federal Tax Information;

(5) Individually Identifiable Health Information as related to HIPAA, Texas HIPAA and Personal Identifying Information under the Texas Identity Theft Enforcement and Protection Act;

(6) Social Security Administration Data, including, without limitation, Medicaid information;

(7) All privileged work product;

(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

"Legally Authorized Representative" of the Individual, as defined by Texas law, including as provided in 45 CFR 435.923 (Medicaid); 45 CFR 164.502(g)(1) (HIPAA); Tex. Occ. Code § 151.002(6); Tex. H. & S. Code §166.164; and Estates Code Ch. 752.

ARTICLE 3.
CONTRACTOR'S DUTIES REGARDING CONFIDENTIAL INFORMATION

3.01 Obligations of CONTRACTOR

CONTRACTOR agrees that:

(A) CONTRACTOR will exercise reasonable care and no less than the same degree of care CONTRACTOR uses to protect its own confidential, proprietary and trade secret information to prevent any portion of the Confidential Information from being used in

a manner that is not expressly an Authorized Purpose under this DUA or as Required by Law. ***45 CFR 164.502(b)(1); 45 CFR 164.514(d)***

(B) Except as Required by Law, CONTRACTOR will not disclose or allow access to any portion of the Confidential Information to any Person or other entity, other than Authorized User's Workforce or Subcontractors (as defined in ***45 C.F.R. 160.103***) of CONTRACTOR who have completed training in confidentiality, privacy, security and the importance of promptly reporting any Event or Breach to CONTRACTOR's management, to carry out CONTRACTOR's obligations in connection with the Authorized Purpose.

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

All of CONTRACTOR's Authorized Users, Workforce and Subcontractors with access to a state computer system or database will complete a cybersecurity training program certified under Texas Government Code Section 2054.519 by the Texas Department of Information Resources or offered under Texas Government Code Sec. 2054.519(f).

(C) CONTRACTOR will establish, implement and maintain appropriate sanctions against any member of its Workforce or Subcontractor who fails to comply with this DUA, the Base Contract or applicable law. CONTRACTOR will maintain evidence of sanctions and produce it to HHS upon request.***45 C.F.R. 164.308(a)(1)(ii)(C); 164.530(e); 164.410(b); 164.530(b)(1)***

(D) CONTRACTOR will not, except as otherwise permitted by this DUA, disclose or provide access to any Confidential Information on the basis that such act is Required by Law without notifying either HHS or CONTRACTOR's own legal counsel to determine whether CONTRACTOR should object to the disclosure or access and seek appropriate relief. CONTRACTOR will maintain an accounting of all such requests for disclosure and responses and provide such accounting to HHS within 48 hours of HHS' request. ***45 CFR 164.504(e)(2)(ii)(A)***

(E) CONTRACTOR will not attempt to re-identify or further identify Confidential Information or De-identified Information, or attempt to contact any Individuals whose records are contained in the Confidential Information, except for an Authorized Purpose, without express written authorization from HHS or as expressly permitted by the Base Contract. ***45 CFR 164.502(d)(2)(i) and (ii)*** CONTRACTOR will not engage in prohibited marketing or sale of Confidential Information. ***45 CFR 164.501, 164.508(a)(3) and (4); Texas Health & Safety Code Ch. 181.002***

(F) CONTRACTOR will not permit, or enter into any agreement with a Subcontractor to, create, receive, maintain, use, disclose, have access to or transmit Confidential Information to carry out CONTRACTOR's obligations in connection with the Authorized Purpose on behalf of CONTRACTOR, unless Subcontractor agrees to comply

with all applicable laws, rules and regulations. ***45 CFR 164.502(e)(1)(ii); 164.504(e)(1)(i) and (2).***

(G) CONTRACTOR is directly responsible for compliance with, and enforcement of, all conditions for creation, maintenance, use, disclosure, transmission and Destruction of Confidential Information and the acts or omissions of Subcontractors as may be reasonably necessary to prevent unauthorized use. ***45 CFR 164.504(e)(5); 42 CFR 431.300, et seq.***

(H) If CONTRACTOR maintains PHI in a Designated Record Set which is Confidential Information and subject to this Agreement, CONTRACTOR will make PHI available to HHS in a Designated Record Set upon request. CONTRACTOR will provide PHI to an Individual, or Legally Authorized Representative of the Individual who is requesting PHI in compliance with the requirements of the HIPAA Privacy Regulations. CONTRACTOR will release PHI in accordance with the HIPAA Privacy Regulations upon receipt of a valid written authorization. CONTRACTOR will make other Confidential Information in CONTRACTOR's possession available pursuant to the requirements of HIPAA or other applicable law upon a determination of a Breach of Unsecured PHI as defined in HIPAA. CONTRACTOR will maintain an accounting of all such disclosures and provide it to HHS within 48 hours of HHS' request. ***45 CFR 164.524and 164.504(e)(2)(ii)(E).***

(I) If PHI is subject to this Agreement, CONTRACTOR will make PHI as required by HIPAA available to HHS for review subsequent to CONTRACTOR's incorporation of any amendments requested pursuant to HIPAA. ***45 CFR 164.504(e)(2)(ii)(E) and (F).***

(J) If PHI is subject to this Agreement, CONTRACTOR will document and make available to HHS the PHI required to provide access, an accounting of disclosures or amendment in compliance with the requirements of the HIPAA Privacy Regulations. ***45 CFR 164.504(e)(2)(ii)(G) and 164.528.***

(K) If CONTRACTOR receives a request for access, amendment or accounting of PHI from an individual with a right of access to information subject to this DUA, it will respond to such request in compliance with the HIPAA Privacy Regulations. CONTRACTOR will maintain an accounting of all responses to requests for access to or amendment of PHI and provide it to HHS within 48 hours of HHS' request. ***45 CFR 164.504(e)(2).***

(L) CONTRACTOR will provide, and will cause its Subcontractors and agents to provide, to HHS periodic written certifications of compliance with controls and provisions relating to information privacy, security and breach notification, including without limitation information related to data transfers and the handling and disposal of Confidential Information. ***45 CFR 164.308; 164.530(c); 1 TAC 202.***

(M) Except as otherwise limited by this DUA, the Base Contract, or law applicable to the Confidential Information, CONTRACTOR may use PHI for the proper management and administration of CONTRACTOR or to carry out CONTRACTOR's

legal responsibilities. Except as otherwise limited by this DUA, the Base Contract, or law applicable to the Confidential Information, CONTRACTOR may disclose PHI for the proper management and administration of CONTRACTOR, or to carry out CONTRACTOR's legal responsibilities, if: ***45 CFR 164.504(e)(4)(A).***

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

(2) CONTRACTOR obtains reasonable assurances from the person or entity to which the information is disclosed that the person or entity will:

(a)Maintain the confidentiality of the Confidential Information in accordance with this DUA;

(b) Use or further disclose the information only as Required by Law or for the Authorized Purpose for which it was disclosed to the Person; and

(c)Notify CONTRACTOR in accordance with Section 4.01 of any Event or Breach of Confidential Information of which the Person discovers or should have discovered with the exercise of reasonable diligence. ***45 CFR 164.504(e)(4)(ii)(B).***

(N) Except as otherwise limited by this DUA, CONTRACTOR will, if required by law and requested by HHS, use commercially reasonable efforts to use PHI to provide data aggregation services to HHS, as that term is defined in the HIPAA, 45 C.F.R. §164.501 and permitted by HIPAA. ***45 CFR 164.504(e)(2)(i)(B)***

(O) CONTRACTOR will, on the termination or expiration of this DUA or the Base Contract, at its expense, send to HHS or Destroy, at HHS's election and to the extent reasonably feasible and permissible by law, all Confidential Information received from HHS or created or maintained by CONTRACTOR or any of CONTRACTOR's agents or Subcontractors on HHS's behalf if that data contains Confidential Information. CONTRACTOR will certify in writing to HHS that all the Confidential Information that has been created, received, maintained, used by or disclosed to CONTRACTOR, has been Destroyed or sent to HHS, and that CONTRACTOR and its agents and Subcontractors have retained no copies thereof. Notwithstanding the foregoing, HHS acknowledges and agrees that CONTRACTOR is not obligated to send to HHSC and/or Destroy any Confidential Information if federal law, state law, the Texas State Library and Archives Commission records retention schedule, and/or a litigation hold notice prohibit such delivery or Destruction. If such delivery or Destruction is not reasonably feasible, or is impermissible by law, CONTRACTOR will immediately notify HHS of the reasons such delivery or Destruction is not feasible, and agree to extend indefinitely the protections of this DUA to the Confidential Information and limit its further uses and disclosures to the purposes that make the return delivery or Destruction of the Confidential Information not feasible for as long as CONTRACTOR maintains such Confidential Information. ***45 CFR 164.504(e)(2)(ii)(J)***

(P) CONTRACTOR will create, maintain, use, disclose, transmit or Destroy Confidential Information in a secure fashion that protects against any reasonably anticipated threats or hazards to the security or integrity of such information or unauthorized uses. ***45 CFR 164.306; 164.530(c)***

(Q) If CONTRACTOR accesses, transmits, stores, and/or maintains Confidential Information, CONTRACTOR will complete and return to HHS at infosecurity@hhsc.state.tx.us the HHS information security and privacy initial inquiry (SPI) at Attachment 1 . The SPI identifies basic privacy and security controls with which CONTRACTOR must comply to protect HHS Confidential Information. CONTRACTOR will comply with periodic security controls compliance assessment and monitoring by HHS as required by state and federal law, based on the type of Confidential Information CONTRACTOR creates, receives, maintains, uses, discloses or has access to and the Authorized Purpose and level of risk. CONTRACTOR's security controls will be based on the National Institute of Standards and Technology (NIST) Special Publication 800-53. CONTRACTOR will update its security controls assessment whenever there are significant changes in security controls for HHS Confidential Information and will provide the updated document to HHS. HHS also reserves the right to request updates as needed to satisfy state and federal monitoring requirements. ***45 CFR 164.306.***

(R) CONTRACTOR will establish, implement and maintain reasonable procedural, administrative, physical and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of the Confidential Information, and with respect to PHI, as described in the HIPAA Privacy and Security Regulations, or other applicable laws or regulations relating to Confidential Information, to prevent any unauthorized use or disclosure of Confidential Information as long as CONTRACTOR has such Confidential Information in its actual or constructive possession. ***45 CFR 164.308 (administrative safeguards); 164.310 (physical safeguards); 164.312 (technical safeguards); 164.530(c)(privacy safeguards).***

(S) CONTRACTOR will designate and identify, a Person or Persons, as Privacy Official ***45 CFR 164.530(a)(1)*** and Information Security Official, each of whom is authorized to act on behalf of CONTRACTOR and is responsible for the development and implementation of the privacy and security requirements in this DUA. CONTRACTOR will provide name and current address, phone number and e-mail address for such designated officials to HHS upon execution of this DUA and prior to any change. If such persons fail to develop and implement the requirements of the DUA, CONTRACTOR will replace them upon HHS request. ***45 CFR 164.308(a)(2).***

(T) CONTRACTOR represents and warrants that its Authorized Users each have a demonstrated need to know and have access to Confidential Information solely to the minimum extent necessary to accomplish the Authorized Purpose pursuant to this DUA and the Base Contract, and further, that each has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information contained in this DUA. ***45 CFR 164.502; 164.514(d).***

(U) CONTRACTOR and its Subcontractors will maintain an updated, complete, accurate and numbered list of Authorized Users, their signatures, titles and the date they agreed to be bound by the terms of this DUA, at all times and supply it to HHS, as directed, upon request.

(V) CONTRACTOR will implement, update as necessary, and document reasonable and appropriate policies and procedures for privacy, security and Breach of Confidential Information and an incident response plan for an Event or Breach, to comply with the privacy, security and breach notice requirements of this DUA prior to conducting work under the Statement of Work. ***45 CFR 164.308; 164.316; 164.514(d); 164.530(i)(1).***

(W) CONTRACTOR will produce copies of its information security and privacy policies and procedures and records relating to the use or disclosure of Confidential Information received from, created by, or received, used or disclosed by CONTRACTOR for an Authorized Purpose for HHS's review and approval within 30 days of execution of this DUA and upon request by HHS the following business day or other agreed upon time frame. ***45 CFR 164.308; 164.514(d).***

(X) CONTRACTOR will make available to HHS any information HHS requires to fulfill HHS's obligations to provide access to, or copies of, PHI in accordance with HIPAA and other applicable laws and regulations relating to Confidential Information. CONTRACTOR will provide such information in a time and manner reasonably agreed upon or as designated by the Secretary of the U.S. Department of Health and Human Services, or other federal or state law. ***45 CFR 164.504(e)(2)(i)(I).***

(Y) CONTRACTOR will only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form, in accordance with applicable rules, regulations and laws. A secure transmission of electronic Confidential Information *in motion* includes, but is not limited to, Secure File Transfer Protocol (SFTP) or Encryption at an appropriate level. If required by rule, regulation or law, HHS Confidential Information *at rest* requires Encryption unless there is other adequate administrative, technical, and physical security. All electronic data transfer and communications of Confidential Information will be through secure systems. Proof of system, media or device security and/or Encryption must be produced to HHS no later than 48 hours after HHS's written request in response to a compliance investigation, audit or the Discovery of an Event or Breach. Otherwise, requested production of such proof will be made as agreed upon by the parties. De-identification of HHS Confidential Information is a means of security. With respect to de-identification of PHI, "secure" means de-identified according to HIPAA Privacy standards and regulatory guidance. ***45 CFR 164.312; 164.530(d).***

(Z) For each type of Confidential Information CONTRACTOR creates, receives, maintains, uses, discloses, has access to or transmits in the performance of the Statement of Work, CONTRACTOR will comply with the following laws rules and regulations, only to the extent applicable and required by law:

- Title 1, Part 10, Chapter 202, Subchapter B, Texas Administrative Code;

- The Privacy Act of 1974;
- OMB Memorandum 07-16;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) as defined in the DUA;
- Internal Revenue Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies;
- National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- NIST Special Publications 800-53 and 800-53A – Recommended Security Controls for Federal Information Systems and Organizations, as currently revised;
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems;
- NIST Special Publication 800-88, Guidelines for Media Sanitization;
- NIST Special Publication 800-111, Guide to Storage of Encryption Technologies for End User Devices containing PHI; and

Any other State or Federal law, regulation, or administrative rule relating to the specific HHS program area that CONTRACTOR supports on behalf of HHS.

(AA) Notwithstanding anything to the contrary herein, CONTRACTOR will treat any Personal Identifying Information it creates, receives, maintains, uses, transmits, destroys and/or discloses in accordance with Texas Business and Commerce Code, Chapter 521 and other applicable regulatory standards identified in Section 3.01(Z), and Individually Identifiable Health Information CONTRACTOR creates, receives, maintains, uses, transmits, destroys and/or discloses in accordance with HIPAA and other applicable regulatory standards identified in Section 3.01(Z).

ARTICLE 4.
BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS

4.01 Breach or Event Notification to HHS. 45 CFR 164.400-414.

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

(B) CONTRACTOR'S obligation begins at the Discovery of an Event or Breach and continues as long as related activity continues, until all effects of the Event are mitigated to HHS's reasonable satisfaction (the "incident response period"). ***45 CFR 164.404.***

(C) Breach Notice:

(1) Initial Notice.

(a) For federal information, including without limitation, Federal Tax Information, Social Security Administration Data, and Medicaid Client Information, within the first, consecutive clock hour of Discovery, and for all other types of Confidential Information not more than 24 hours after Discovery, or in a timeframe otherwise approved by HHS in writing, initially report to HHS's Privacy and Security Officers via email at: privacy@HHSC.state.tx.us and to the HHS division responsible for this DUA; and IRS Publication 1075; Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a; OMB Memorandum 07-16 as cited in HHSC-CMS Contracts for information exchange.

(b) Report all information reasonably available to CONTRACTOR about the Event or Breach of the privacy or security of Confidential Information. ***45 CFR 164.410.***

(c) Name, and provide contact information to HHS for, CONTRACTOR's single point of contact who will communicate with HHS both on and off business hours during the incident response period.

(2) Formal Notice. No later than two business days after the Initial Notice above, provide formal notification to privacy@HHSC.state.tx.us and to the HHS division responsible for this DUA, including all reasonably available information about the Event or Breach, and CONTRACTOR's investigation, including without limitation and to the extent available***: For (a) - (m) below: 45 CFR 164.400-414.***

(a) The date the Event or Breach occurred;

(b) The date of CONTRACTOR's and, if applicable, Subcontractor's Discovery;

(c) A brief description of the Event or Breach; including how it occurred and who is responsible (or hypotheses, if not yet determined);

(d) A brief description of CONTRACTOR's investigation and the status of the investigation;

(e) A description of the types and amount of Confidential Information involved;

(f) Identification of and number of all Individuals reasonably believed to be affected, including first and last name of the Individual and if applicable the, Legally Authorized Representative, last known address, age, telephone number, and email address if it is a preferred contact method, to the extent known or can be reasonably determined by CONTRACTOR at that time;

(g) CONTRACTOR's initial risk assessment of the Event or Breach demonstrating whether individual or other notices are required by applicable law or this DUA for HHS approval, including an analysis of whether there is a low probability of compromise of the Confidential Information or whether any legal exceptions to notification apply;

(h) CONTRACTOR's recommendation for HHS's approval as to the steps Individuals and/or CONTRACTOR on behalf of Individuals, should take to protect the Individuals from potential harm, including without limitation CONTRACTOR's provision of notifications, credit protection, claims monitoring, and any specific protections for a Legally Authorized Representative to take on behalf of an Individual with special capacity or circumstances;

(i) The steps CONTRACTOR has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);

(j) The steps CONTRACTOR has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Event or Breach;

(k) Identify, describe or estimate the Persons, Workforce, Subcontractor, or Individuals and any law enforcement that may be involved in the Event or Breach;

(l) A reasonable schedule for CONTRACTOR to provide regular updates during normal business hours to the foregoing in the future for response to the Event or Breach, but no less than every three (3) business days or as otherwise directed by HHS, including information about risk estimations, reporting, notification, if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and

(m) Any reasonably available, pertinent information, documents or reports related to an Event or Breach that HHS requests following Discovery.

4.02 Investigation, Response and Mitigation. 45 CFR 164.308, 310 and 312; 164.530

(A) CONTRACTOR will immediately conduct a full and complete investigation, respond to the Event or Breach, commit necessary and appropriate staff and resources to expeditiously respond, and report as required to and by HHS for incident response purposes and for purposes of HHS's compliance with report and notification requirements, to the reasonable satisfaction of HHS.

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

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

(D) CONTRACTOR will fully cooperate with HHS's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such Event or Breach, or to recover or protect any Confidential Information, including complying with reasonable corrective action or measures, as specified by HHS in a Corrective Action Plan if directed by HHS under the Base Contract.

4.03 Breach Notification to Individuals and Reporting to Authorities. Tex. Bus. & Comm. Code §521.053; 45 CFR 164.404 (Individuals), 164.406 (Media); 164.408 (Authorities)

(A) HHS may direct CONTRACTOR to provide Breach notification to Individuals, regulators or third-parties, as specified by HHS following a Breach.

(B) CONTRACTOR shall give HHS an opportunity to review and provide feedback to CONTRACTOR and to confirm that CONTRACTOR's notice meets all regulatory requirements regarding the time, manner and content of any notification to Individuals, regulators or third-parties, or any notice required by other state or federal authorities. HHS shall have ten (10) business days to provide said feedback to CONTRACTOR. Notice letters will be in CONTRACTOR's name and on CONTRACTOR's letterhead, unless otherwise directed by HHS, and will contain contact information, including the name and title of CONTRACTOR's representative, an email address and a toll-free telephone number, if required by applicable law, rule, or regulation, for the Individual to obtain additional information.

(C) CONTRACTOR will provide HHS with copies of distributed and approved communications.

(D) CONTRACTOR will have the burden of demonstrating to the reasonable satisfaction of HHS that any notification required by HHS was timely made. If there are delays outside of CONTRACTOR's control, CONTRACTOR will provide written documentation of the reasons for the delay.

(E) If HHS delegates notice requirements to CONTRACTOR, HHS shall, in the time and manner reasonably requested by CONTRACTOR, cooperate and assist with CONTRACTOR's information requests in order to make such notifications and reports.

ARTICLE 5.
STATEMENT OF WORK

"Statement of Work" means the services and deliverables to be performed or provided by CONTRACTOR, or on behalf of CONTRACTOR by its Subcontractors or agents for HHS that are described in detail in the Base Contract. The Statement of Work, including any future amendments thereto, is incorporated by reference in this DUA as if set out word-for-word herein.

ARTICLE 6.
GENERAL PROVISIONS

6.01 Oversight of Confidential Information

CONTRACTOR acknowledges and agrees that HHS is entitled to oversee and monitor CONTRACTOR's access to and creation, receipt, maintenance, use, disclosure of the Confidential Information to confirm that CONTRACTOR is in compliance with this DUA.

6.02 HHS Commitment and Obligations

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

6.03 HHS Right to Inspection

At any time upon reasonable notice to CONTRACTOR, or if HHS determines that CONTRACTOR has violated this DUA, HHS, directly or through its agent, will have the right to inspect the facilities, systems, books and records of CONTRACTOR to monitor compliance with this DUA. For purposes of this subsection, HHS's agent(s) include, without limitation, the HHS Office of the Inspector General or the Office of the Attorney General of Texas, outside consultants or legal counsel or other designee.

6.04 Term; Termination of DUA; Survival

This DUA will be effective on the date on which CONTRACTOR executes the DUA, and will terminate upon termination of the Base Contract and as set forth herein. If the Base Contract is extended or amended, this DUA shall be extended or amended concurrent with such extension or amendment.

(A) HHS may immediately terminate this DUA and Base Contract upon a material violation of this DUA.

(B) Termination or Expiration of this DUA will not relieve CONTRACTOR of its obligation to return or Destroy the Confidential Information as set forth in this DUA and to continue to safeguard the Confidential Information until such time as determined by HHS.

(C) If HHS determines that CONTRACTOR has violated a material term of this DUA; HHS may in its sole discretion:

(1) Exercise any of its rights including but not limited to reports, access and inspection under this DUA and/or the Base Contract; or

(2) Require CONTRACTOR to submit to a Corrective Action Plan, including a plan for monitoring and plan for reporting, as HHS may determine necessary to maintain compliance with this DUA; or

(3) Provide CONTRACTOR with a reasonable period to cure the violation as determined by HHS; or

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

Before exercising any of these options, HHS will provide written notice to CONTRACTOR describing the violation, the requested corrective action CONTRACTOR may take to cure the alleged violation, and the action HHS intends to take if the alleged violated is not timely cured by CONTRACTOR.

(D) If neither termination nor cure is feasible, HHS shall report the violation to the Secretary of the U.S. Department of Health and Human Services.

(E) The duties of CONTRACTOR or its Subcontractor under this DUA survive the expiration or termination of this DUA until all the Confidential Information is Destroyed or returned to HHS, as required by this DUA.

6.05 Governing Law, Venue and Litigation

(A) The validity, construction and performance of this DUA and the legal relations among the Parties to this DUA will be governed by and construed in accordance with the laws of the State of Texas.

(B) The Parties agree that the courts of Texas, will be the exclusive venue for any litigation, special proceeding or other proceeding as between the parties that may be brought, or arise out of, or in connection with, or by reason of this DUA.

6.06 Injunctive Relief

(A) CONTRACTOR acknowledges and agrees that HHS may suffer irreparable injury if CONTRACTOR or its Subcontractor fails to comply with any of the terms of this DUA with respect to the Confidential Information or a provision of HIPAA or other laws or regulations applicable to Confidential Information.

(B) CONTRACTOR further agrees that monetary damages may be inadequate to compensate HHS for CONTRACTOR's or its Subcontractor's failure to comply. Accordingly, CONTRACTOR agrees that HHS will, in addition to any other remedies available to it at law or in equity, be entitled to seek injunctive relief without posting a bond and without the necessity of demonstrating actual damages, to enforce the terms of this DUA.

6.07 Responsibility.

To the extent permitted by the Texas Constitution, laws and rules, and without waiving any immunities or defenses available to CONTRACTOR as a governmental entity, CONTRACTOR shall be solely responsible for its own acts and omissions and the acts and omissions of its employees, directors, officers, Subcontractors and agents. HHS shall be solely responsible for its own acts and omissions.

6.08 Insurance

(A) As a governmental entity, and in accordance with the limits of the Texas Tort Claims Act, Chapter 101 of the Texas Civil Practice and Remedies Code, CONTRACTOR either maintains commercial insurance or self-insures with policy limits in an amount sufficient to cover CONTRACTOR's liability arising under this DUA. CONTRACTOR will request that HHS be named as an additional insured. HHSC reserves the right to consider alternative means for CONTRACTOR to satisfy CONTRACTOR's financial responsibility under this DUA. Nothing herein shall relieve CONTRACTOR of its financial obligations set forth in this DUA if CONTRACTOR fails to maintain insurance.

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

6.08 Fees and Costs

Except as otherwise specified in this DUA or the Base Contract, if any legal action or other proceeding is brought for the enforcement of this DUA, or because of an alleged dispute, contract violation, Event, Breach, default, misrepresentation, or injunctive action, in connection with any of the provisions of this DUA, each party will bear their own legal expenses and the other cost incurred in that action or proceeding.

6.09 Entirety of the Contract

This DUA is incorporated by reference into the Base Contract as an amendment thereto and, together with the Base Contract, constitutes the entire agreement between the parties. No change, waiver, or discharge of obligations arising under those documents will be valid unless in writing and executed by the party against whom such change, waiver, or discharge is sought to be

enforced. If any provision of the Base Contract, including any General Provisions or Uniform Terms and Conditions, conflicts with this DUA, this DUA controls.

6.10 Automatic Amendment and Interpretation

If there is (i) a change in any law, regulation or rule, state or federal, applicable to HIPPA and/or Confidential Information, or (ii) any change in the judicial or administrative interpretation of any such law, regulation or rule,, upon the effective date of such change, this DUA shall be deemed to have been automatically amended, interpreted and read so that the obligations imposed on HHS and/or CONTRACTOR remain in compliance with such changes. Any ambiguity in this DUA will be resolved in favor of a meaning that permits HHS and CONTRACTOR to comply with HIPAA or any other law applicable to Confidential Information.

TEXAS Health and Human Services

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 #:

Attachment B
Checklist for Death Record Data - COVID
March 2020 and beyond

Instructions:

1. Since these data are confidential, all requested certificate items need to have brief justifications according to your project aims.
2. If a certificate item is used for linkage, then state how and whether it will be removed from the resulting linked analysis file. If the certificate item will be retained in the linked analysis file, please also provide a brief justification according to your project aims.
3. For certain sensitive data elements, such as certificate number or residence address, consider alternative means of accomplishing your project aims while using less sensitive data. Examples include creating your own unique identifier instead of requesting the certificate number and requesting geocoded census tracts instead of residence address.

I. Death Certificate Items

✓	Item Number	Item Descriptor	Justification
☐	n/a	State File Number (Certificate Number)	
☒	n/a	State of Death	Helps determine if death occurred in region or if the death occurred elsewhere
☒ ☒ ☒ ☒ ☒ ☐	1.	Legal Name of Deceased: First Middle Last Maiden Suffix	Case investigation
☐ ☐ ☐ ☐	1.	Deceased AKA's if any: First Middle Last	
☒ ☐	2.	Date of Death Date of Death Type (Actual, Presumed, Estimated, Found)	case investigation and surveillance
☒	3.	Sex	case investigation and surveillance
☒	4.	Date of Birth	case investigation and surveillance
☒	5.	Age - Last Birthday	case investigation and surveillance
☒		Age – kind of units (years, months, weeks, days, hours, minutes)	case investigation and surveillance
☐ ☐	6.	Birthplace -City State or Foreign Country	
☐	8.	Marital Status at Time of Death	
☐ ☐ ☐ ☐ ☐	9.	Surviving Spouse (If wife, give name prior to first marriage): First Middle Last Suffix	
☒	10a.	Residence Street Address	Case investigation
☒	10b.	Apt No	Case investigation
☒	10c.	City or Town of Residence	Case investigation and surveillance
☒	10d.	County of Residence	Helps determine if the death was among a resident of the region
☒	10e.	State of Residence	Helps determine if the death was among a resident of the region
☒ ☐	10f.	Zip Code Zip Code Extension	Case investigation and surveillance

✓	Item Number	Item Descriptor	Justification
☐	10g.	Inside City Limits?	
☐	11.	Father's Name:	
☐		First	
☐		Middle	
☐		Last	
☐		Suffix	
☐	12.	Mother's Name Prior to First Marriage:	
☐		First	
☐		Middle	
☐		Last	
☐		Suffix	
☒	13.	Place of Death:	Case investigation and surveillance
		If Death Occurred in a Hospital: Inpatient	
		If Death Occurred in a Hospital: ER/Outpatient	
		If Death Occurred in a Hospital: DOA	
		If Death Occurred Somewhere Other Than a Hospital: Hospice Facility	
		If Death Occurred Somewhere Other Than a Hospital: Nursing Home (*Includes LTC)*	
		If Death Occurred Somewhere Other Than a Hospital: Decedent's Home	
☐		Other	
		Other (Specify)	
☒	14.	County of Death	Helps determine if death occurred in region or if the death occurred elsewhere
☒	15.	City/Town of Death (If outside city limits give precinct no)	Case investigation and surveillance
☐		Street Address	
☐		Zip Code	
☐		Zip Code Extension	
☒	16.	Facility Name (If not institution give street address)	Case investigation
☐	17.	Informant's Name &	
☐		Relationship to Deceased	
	18.	Mailing Address of Informant:	
☐		Street	
☐		Number	
☐		City	
☐		State	
☐		Zip Code	
☐		Zip Code Extension	
☐	19.	Method of Disposition:	
		Burial	
		Cremation	
		Donation	
		Entombment	
		Removal From State	
		Other	
☐		Other (Specify)	
☐	20.	License Number of Funeral Director or Person Acting As Such	
☐	21.	Section	
☐		Block	
☐		Lot	
☐		Space	
☐		Unknown	
☐	22.	Place of Disposition (Name of cemetery, crematory, other place)	

✓	Item Number	Item Descriptor	Justification
☐	23.	Location of Disposition: City, Town State	
☐	24.	Name of Funeral Facility	
	25.	Complete Address of Funeral Facility: Street Number City State Zip Code Zip Code Extension	
☒	26.	Certifier: Certifying Physician Medical Examiner Justice of the Peace	Case investigation
☐	28.	Date Certified (Mo/Day/Yr)	
☐	29.	Certifier's License Number	
☐	30.	Time of Death Time of Death Type (Actual, Presumed, Estimated, Found)	
☒	31.	Certifier's Address: Street and Number City State Zip Code Zip Code Extension	Case investigation
☐	32.	Title of Certifier	
	33.	Chain of Events –Diseases, Injuries or Complications – That Directly Caused the Death: *(if you want to order ICD-10 codes, check with the Section II of this checklist):*	
☒	33. Part 1a.	Cause of Death A (Immediate Cause) – *certifier's text* Approximate Interval: Onset to death	Case investigation and surveillance
☒	33. Part 1b.	Cause of Death B - *certifier's text* Approximate Interval: Onset to death	Case investigation and surveillance
☒	33. Part 1c.	Cause of Death C - *certifier's text* Approximate Interval: Onset to death	Case investigation and surveillance
☒	33. Part 1d.	Cause of Death D - *certifier's text* Approximate Interval: Onset to death	Case investigation and surveillance
☒	33. Part 2.	Other Significant Conditions Contributing to Death but not Resulting in the Underlying Cause Given in Part 1.	Case investigation and surveillance
☒	34.	Was an Autopsy Performed?	Case investigation and surveillance
☐	35.	Were Autopsy Findings Available to Complete the Cause of Death?	
☐	36.	Manner of Death	
☐	37.	Did Tobacco Contribute to Death?	
☐	38.	If Female: Not pregnant within past year Pregnant at time of death Not pregnant, but pregnant within 42 days of death Not pregnant, but pregnant 43 days to 1 year before death Unknown if pregnant within the past year	
☐	39.	If Transportation Injury, Specify: Driver/Operator Passenger Pedestrian Other	

✓	Item Number	Item Descriptor	Justification
☐		Other (Specify)	
☐	40a.	Date of Injury (Mo/Day/Yr)	
☐	40b.	Time of Injury	
☐	40c.	Injury at Work?	
☐	40d.	Place of Injury (e.g. Decedent's home; construction site, restaurant, wooded area)	
☐ ☐ ☐ ☐ ☐	40e.	Location: Street Number City State Zip Code	
☐	40f.	County of Injury	
☐	41.	Describe How Injury Occurred	
☐	43.	Decedent's Education	
	44.	Decedent of Hispanic Origin?	
☒		No, Not Spanish, Hispanic/Latino	Case investigation and surveillance
☒		Yes, Mexican, Mexican American, Chicano	Case investigation and surveillance
☒		Yes, Puerto Rican	Case investigation and surveillance
☒		Yes, Cuban	Case investigation and surveillance
☒		Yes, Other Spanish/Hispanic/Latino	Case investigation and surveillance
☒		Specify	Case investigation and surveillance
	45.	Decedent's Race *(2006 revision allows informants to select one or more races to indicate what the decedent considered himself or herself to be):*	
☒		White	Case investigation and surveillance
☒		Black or African American	Case investigation and surveillance
☒ ☒		American Indian or Alaska Native Name of the enrolled or principal tribe	Case investigation and surveillance
☒		Asian Indian	Case investigation and surveillance
☒		Chinese	Case investigation and surveillance
☒		Filipino	Case investigation and surveillance
☒		Japanese	Case investigation and surveillance
☒		Korean	Case investigation and surveillance
☒		Vietnamese	Case investigation and surveillance
☒		Other Asian	Case investigation and surveillance
☒		Other Asian (Specify)	Case investigation and surveillance
☒		Native Hawaiian	Case investigation and surveillance
☒		Guamanian or Chamorro	Case investigation and surveillance
☒		Samoan	Case investigation and surveillance
☒		Other Pacific Islander	Case investigation and surveillance
☒		Other Pacific Islander (Specify)	Case investigation and surveillance
☒		Other	Case investigation and surveillance
☒		Other (Specify)	Case investigation and surveillance
☐	46.	Ever in U.S. Armed Forces?	
☐	47.	Ever a Peace Officer in This State?	
☒	48.	Decedent's Usual Occupation (Indicate type of work done during most of working life).	Case investigation and surveillance
☐	49.	Decedent's Type of Business/Industry	
☐ ☐ ☐	n/a	If Deceased Served in U.S. Armed Forces, Fill Out the Following: Is the deceased reported to have been in such service? Name of organization in which service was rendered?	

✓	Item Number	Item Descriptor	Justification
☐ ☐		Serial number of discharge papers or adjusted service certificate? Name of next of kin or of next friend? Post Office Address?	

II. Other Variables Calculated Based on the Death Record Items

✓	Item Number	Item Descriptor	
☐		Record Type *(Identified, Un-indentified, Out of State, Catastrophic)*	
☐		Age Group	
☐		Additional Funeral Home	
☒		Causes of Death (multiple, including underlying) – *ICD-10 codes*	Case investigation and surveillance (may not yet be present in the record)
☒		Underlying Cause of Death – *ICD-10 codes*	Case investigation and surveillance (may not yet be present in the record)
☐		CDC 113 Selected Causes of Death (ICD-10)	
☐		CDC 130 Selected Causes of Infant Death (ICD-10)	
☐		Was Death a Result of an Injury?	
☒		Decedent's Bridged Race Code *(determined by NCHS)*	Case investigation and surveillance (may not yet be present in the record)
☒		Decedent's Race/Ethnicity *(based on the TSDC method)*	
☒		Decedent's Spanish/Hispanic/Latino Origin Unknown	
☒		Decedent's Race: Unknown	
☐		Longitude *(based on decedent's street address)*	
☐		Latitude *(based on decedent's street address)*	
☐		GIS Match code	
☐		GIS Location code	
☐		Geocoding accuracy	
☐		1990 census tract *(based on decedent's street address)*	
☐		2000 census tract *(based on decedent's street address)*	
☐		2010 census tract *(based on decedent's street address)*	
☐		Zip code tabulation areas (ZCTAs) - from 2013 data	
☐		GIS Residence County Name - from 2014 data	
☐		GIS Residence County FIPS - from 2014 data	

Last updated: March 20, 2018

ATTACHMENT C

LIST OF INDIVIDUALS ACCESSING VITAL EVENTS DATA

Submit list of program staff's name and job titles of all staff who will have access to these data within ten days of execution.

For the duration of this agreement, Contractor must maintain a list of named employees who will utilize this data. Any addition or deletion of names to this list must be updated and maintained by Contractor, and this list must be made available immediately to DSHS upon their request. The parties acknowledge that this list may be updated frequently. When an updated list is requested by DSHS, please send a revised version, including a description of who was removed and/or added to the list, to HIRBRequests@dshs.texas.gov and reference the agreement number. After review of the revised list by the DSHS Contract Manager, this updated list will beincorporated
into the agreement as an attachment and become effective upon transmittal of the DSHS Contract Manager's acceptance, which may be provided by email.

CURRENT LIST as of 9/21/2020

Name	Title
Jacqueline Johnson-Minter, MD, MPH, MBA	Fort Bend County Health and Human Services Director and Local Health Authority
Kaye Reynolds, DrPH	Deputy Director for Public Health Practice
Nicolette Janoski, MPH, CEM	Epidemiology Program Manager
Catalina Lozano	Epidemiologist
Maureen Crespo, RN	Public Health Nurse