DATA USE AGREEMENT
BETWEEN HEALTH AND HUMAN SERVICES COMMISSION
AND
_____ Denton Independent School District _____ ("CONTRACTOR")

STATE OF TEXAS

COUNTY OF TRAVIS

DATA USE AGREEMENT
BETWEEN HEALTH AND HUMAN SERVICES COMMISSION
AND
Denton Independent School District ("CONTRACTOR")

This Data Use Agreement ("DUA"), effective as of the date signed below ("Effective Date"), is entered into by and between Health and Human Services Commission ("HHSC") and Denton Independent School District ("CONTRACTOR"), and incorporated into the terms of the "Base Contract" entered into by these parties, HHSC Contract No. _____.

ARTICLE 1. PURPOSE

CONTRACTOR must create, receive, maintain, or have access to information about HHSC programs and/or its clients for HHSC program benefits and services, as described in the Base Contract. This information is deemed confidential under the Base Contract and state and federal law. CONTRACTOR acknowledges the sensitive and confidential nature of this information and agrees that it will take all necessary and reasonable measures to preserve and protect the confidentiality, privacy, security, integrity, and availability of the HHSC information.

The purpose of this DUA is to facilitate creation, receipt, maintenance and access to Confidential Information with CONTRACTOR, and clarify CONTRACTOR's obligations with respect to the Confidential Information. This DUA expressly describes the limited purposes for which the CONTRACTOR may create, receive, maintain, or have access to Confidential Information, and establishes CONTRACTOR's rights and responsibilities concerning the information. This DUA also describes HHSC's remedies in the event of CONTRACTOR's noncompliance with its obligations under this DUA.

As of the Effective Date of this DUA, if Article 10, Section 16.01 of HHSC's UNIFORM TERMS AND CONDITIONS conflicts with this DUA, this DUA controls.

ARTICLE 2. DEFINITIONS

For the purposes of this DUA, the following terms below have the meanings set forth below.

Section 2.01 ***Definition of Confidential Information***

For the purposes of this DUA, the term "Confidential Information" and other terms have the meaning set forth below. Capitalized terms included have the meanings set forth in Section 2.02 below.

"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) 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 as defined by Texas Business and Commerce Code Ch. 521;

(4) Federal Tax Information;

(5) Personally Identifiable Information;

(6) Social Security Administration Data;

(7) All non-public budget, expense, payment and other financial information;

(8) All privileged work product;

(9) All information designated as confidential under the laws of the State of Texas and of the United States;

(10) To the extent permitted under the laws and constitution of the State of Texas, all information designated by HHSC or any other State agency as confidential, including but not limited all information designated as confidential under the Texas Public Information Act, Texas Government Code, Chapter 552;

(11) Information that CONTRACTOR has access to or that is created, utilized, developed, received, or maintained by HHSC, the CONTRACTOR, or participating State agencies for the purpose of fulfilling a duty or obligation under this DUA and that has not been publicly disclosed;

(12) Information identified in Attachment 6 attached to this DUA and to which CONTRACTOR specifically seeks to obtain access for an Authorized Purpose.

Section 2.02 ***Other Definitions***

For the purposes of this DUA, the following terms have the meanings set forth below.

"Authorized Purpose" means the specific purpose or purposes described in the **Scope of Work** of the Base Contract for Contractor to fulfill its obligations under the Base Contract, or any other purpose expressly authorized by HHSC 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 know and 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, such agreement evidenced by each Authorized User's signature on the form attached to this DUA as Attachment 8.

"Business Associate" means a Person or organization, other than a member of HHSC's workforce, that performs, on behalf of HHSC, certain functions, activities, or services that create, receive, maintain, have access to or transmit Protected Health Information ("PHI") such as without limitation activities listed in the HIPAA definition and regulation of Business Associates. CONTRACTOR and CONTRACTOR's Subcontractor(s), to the extent applicable to the Base Contract, are "Business Associates" of HHSC for purposes of this DUA, if a Business Associate subcontracts part of its business associate function requiring the Subcontractor to create, receive, maintain, have access to or transmit PHI, except to the extent Contractors are on an HHSC site and treated as Workforce or are conduits as described by HIPAA. "Business Associate" excludes a mere conduit that does not require access to PHI. Business Associates are entities, for example and without limitation and to the extent applicable to the Base Contract: entities that provide data transmission services to HHSC and require access on a routine basis to PHI; entities that offer a personal health record on behalf of a covered entity; a Subcontractor, if a business associate subcontracts part of its

function subject to this Agreement; a Person who creates, receives, maintains or transmits PHI on behalf of HHSC; or physical storage facilities or companies that store paper or electronic PHI. Business Associates do not include entities, for example and without limitation and to the extent applicable to the Base Contract: a telecommunications company or mail courier without regular access to PHI. The meaning, application of and regulation of Business Associates are more fully described in the HIPAA Privacy, Security and Breach Regulations.

"Breach" means any unauthorized acquisition, access, use, or disclosure of Confidential Information in a manner not permitted by this DUA, the Base Contract or applicable law. Additionally:

(1) **HIPAA Breach of PHI**. With respect to Protected Health Information ("PHI") pursuant to HIPAA Privacy and Breach Notification Regulations and regulatory guidance, any unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Regulations is presumed to be a Breach unless CONTRACTOR, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Compromise will be determined by a documented Risk Assessment including at least the following factors:

1. The nature and extent of the Confidential Information involved, including the types of identifiers and the likelihood of re-identification of PHI;
2. The unauthorized person who used or to whom PHI was disclosed;
3. Whether the Confidential Information was actually acquired or viewed; and
4. The extent to which the risk to PHI has been mitigated.

With respect to PHI, a "breach," pursuant to HIPAA Breach Regulations and regulatory guidance excludes:

(A) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of HHSC or CONTRACTOR if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Regulations.

(B) Any inadvertent disclosure by a person who is authorized to access PHI at HHSC or CONTRACTOR to another person authorized to access PHI at the same HHSC or CONTRACTOR location, or organized health care arrangement, as defined by, in which HHSC participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Regulations.

(C) A disclosure of PHI where CONTRACTOR demonstrates a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information, pursuant to HIPAA Breach Regulations and regulatory guidance.

(2) **Texas Breach**. Breach means "Breach of System Security," applicable to electronic Sensitive Personal Information (SPI) as defined by the Texas Breach Law. The currently undefined phrase in the Texas Breach Law, "compromises the security, confidentiality, or integrity of sensitive personal information," will be interpreted in HHSC's sole discretion, including without limitation, directing CONTRACTOR to document a Risk Assessment of any reasonably likelihood of harm or loss to an individual, taking into consideration relevant fact-specific information about the breach, including without limitation, any legal requirements the unauthorized person is subject to regarding Confidential Information to protect and further safeguard the data from unauthorized use or disclosure, or the receipt of satisfactory assurance from the person that the person

agrees to further protect and safeguard, return and/or destroy the data to the satisfaction of HHSC. Breached SPI that is also PHI will be considered a HIPAA breach, to the extent applicable.

(3) Any unauthorized use or disclosure as defined by any other law and any regulations adopted there under regarding Confidential Information.

"Client Information" means Personally Identifiable Information about or concerning recipients of benefits under one or more public assistance programs administered by HHSC.

"De-Identified Information" means health information, as defined in the HIPAA Privacy Regulations as not PHI, regarding which there is no reasonable basis to believe that the information can be used to identify an Individual. HHSC has determined that health information is not individually identifiable and there is no reasonable basis to believe that the information can be used to identify an individual only if:

(1) The following identifiers of the Individual or of relatives, employers, or household members of the individual, are removed from the information:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(i) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(ii) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an Individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers (including without limitation, Medicaid Identification Number);

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (C) of this section; and

(2**)** Neither HHSC nor CONTRACTOR has actual knowledge that the information could be used alone or in combination with other information to identify an Individual who is a subject of the information."

"Designated Record Set" means a group of records maintained by or for a covered entity that is: (i) the medical records and billing records about Individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals. For purposes of this definition, "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

"Destroy" for Confidential Information means, as specified in the HIPAA Security Rule Regulations:

(1) Paper, film, or other hard copy media have been shredded or destroyed such that the Confidential Information without limitation including PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

(2) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization," such that the Confidential Information without limitation including PHI cannot be retrieved.

"Discovery" means the first day on which an Event or Breach becomes known to CONTRACTOR, or, by exercising reasonable diligence would have been known to CONTRACTOR, and includes Events or Breaches discovered by or reported to CONTRACTOR by its officers, directors, employees, agents, work force members, Subcontractors or third-parties (such as legal authorities and/or Individuals).

"Electronic Health Record" means an electronic record of health-related information on an Individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

"Electronic Protected Health Information" ("EPHI") means any PHI which is maintained or transmitted by "Electronic Media" as defined in HIPAA, 45 C.F.R. §160.102.

"Encryption" of Confidential Information means, as described in HIPAA, 45 C.F.R. §164.304 of the HIPAA Security Regulations, the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been Breached. To avoid a Breach of the confidential process or key, these decryption tools will be stored on a device or at a location separate from the data they are used to encrypt or decrypt.

"Event" means a potential, suspected or attempted unauthorized access, use, disclosure, modification, loss or destruction of Confidential Information, which has the potential for jeopardizing the confidentiality, integrity or availability of the Confidential Information, but excludes completed, unsuccessful hacking events using common tools such as PING, netstat, telnet, tracert, etc. An **Event** becomes a **Breach** when the event involves actual unauthorized access, use, disclosure, modification, loss or destruction of Confidential

Information, which has the potential for jeopardizing the confidentiality, integrity or availability of the Confidential Information.

"Federal Tax Information" has the meaning assigned in the Internal Revenue Code, Title 26 of the United States Code and regulations adopted under that code.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as amended by the HITECH ACT and regulations thereunder including without limitation HIPAA Omnibus Rules, in 45 CFR Parts 160 and 164. Public Law 104-191 (42 U.S.C. §1320d, *et seq.*); Public Law 111-5 (42 U.S.C. §13001 *et. seq.*); including without limitation regulations and guidance issued by the Secretary, such as 65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 74 FR 19006, April 27, 2009; 75 FR 40868, July 14, 2010; and 78 FR 5695, Jan. 25, 2013.

"**HIPAA Breach Regulations**" means the HIPAA Breach Notification Regulations codified at 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subpart D relating to unsecured PHI.

"**HIPAA Omnibus Rules**" means the rule modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act; and other modifications published in Federal Register Vol. 78, January 25, 2013 which include:

(1) Final modifications to the HIPAA regulations mandated by the HITECH Act, and certain other modifications of the Rules to improve the HIPAA rules;

(2) Final rule adopting changes to the HIPAA Enforcement Rule;

(3) Final rule on HIPAA Breach Regulations for unsecured PHI under the HITECH Act; and

(4) Final rule modifying the HIPAA Privacy Regulations as required by the Genetic Information Nondiscrimination Act of 2008 (GINA).

"HIPAA Privacy Regulations" means the HIPAA Privacy Regulations codified at 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subpart A, Subpart D and Subpart E.

"HIPAA Security Regulations" means the HIPAA Security Regulations codified at 45 C.F.R. Part 160 and 45 C.F.R. Part 164 Subpart A and Subpart C, and Subpart D.

"HITECH Act" means the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5), and regulations adopted under that act.

"Individual" means the subject of the Confidential Information, including without limitation PHI, and who will include the subject's Legally authorized representative who qualifies under the HIPAA Privacy Regulation as a Legally authorized representative of the Individual wherein HIPAA defers to Texas law for determination, for example, without limitation as provided in Tex. Occ. Code § 151.002(6); Tex. H. & S. Code §166.164; Texas Prob. Code § 3 and Tex. Estates Code §§752.051,752.112.

"Legally authorized representative" of the Individual, as defined by Texas law, for example, without limitation as provided in Tex. Occ. Code § 151.002(6); Tex. H. & S. Code §166.164; Estates Code Ch. 752 and Texas Prob. Code § 3, includes:

(1) A parent or legal guardian if the Individual is a minor;

(2) A legal guardian if the Individual has been adjudicated incompetent to manage the Individual's personal affairs;

(3) An agent of the Individual authorized under a Medical Power of Attorney;

(4) An agent of the Individual authorized under a Durable, Statutory or non-medical Power of Attorney, limited to certain powers over benefits from certain governmental programs, including without limitation Medicaid, as defined by Texas Estates Code §752.112, effective Jan. 1, 2014.

(5) An attorney ad litem appointed for the Individual;

(6) A guardian ad litem appointed for the Individual;

(7) A personal representative or statutory beneficiary if the Individual is deceased;

(8) An attorney retained by the Individual or by another person listed herein;

(9) If an individual is deceased, their personal representative must be the executor, independent executor, administrator, independent administrator, or temporary administrator of the estate; pr

(10) To a state-designated Protection and Advocacy system to the extent that such disclosure is Required by Law and the disclosure complies with the requirements of that law.

"Information Security Guidelines and Procedures" means the information security guidelines, procedures, protocols, and other documents or information identified in Attachment 7 to this DUA.

"Limited Data Set" means PHI that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the individual as defined at 45 CFR 164.514(e)(2):

(1) names;

(2) postal address information, other than town or city, State, and zip code;

(3) telephone numbers;

(4) fax numbers;

(5) electronic mail addresses;

(6) Social Security numbers;

(7) medical record numbers;

(8) health plan beneficiary numbers;

(9) account numbers;

(10) certificate/license numbers;

(11) vehicle identifiers and serial numbers, including license plate numbers;

(12) device identifiers and serial numbers;

(13) web universal resource locators (URLs);

(14) internet protocol (IP) address numbers;

(15) biometric identifiers, including finger and voice prints; and

(16) full face photographic images and any comparable images.

"Person" means without limitation, an employee, agent, representative, firm, corporation, organization, Subcontractor, a member of the general public, or a consumer.

"Personally Identifiable Information" or "PII" means information that can be used to uniquely identify, contact, or locate a single Individual or can be used with other sources to uniquely identify a single Individual.

"Protected Health Information" or "PHI" means individually identifiable health information in any form that is created or received by a HIPAA covered entity, and relates to the individual's healthcare condition, provision of healthcare, or payment for the provision of healthcare, as further described and defined in the HIPAA. PHI includes demographic information unless such information is De-identified, as defined above. PHI includes without limitation, "Electronic Protected Health Information" as defined above, and unsecure PHI. PHI includes PHI of a deceased individual within 50 years of the date of death.

"Required by Law" shall have the same meaning as the term "required by law" in 45 CFR 164.103 but applies to all Confidential Information, not only PHI.

"Scope of Work" means the services and deliverables to be performed or provided by CONTRACTOR, or on behalf of CONTRACTOR by its Subcontractors or agents for HHSC that are described in Attachment 2 attached to this DUA. If the Scope of Work includes or consists of a written proposal by the CONTRACTOR, any conflict between such proposal and the other terms of the Base Contract or this DUA will be resolved, in HHSC's sole discretion, by giving effect to the other terms of the Base Contract or this DUA.

"**Secretary**" means the United States Secretary of the Department of Health and Human Services or designee.

"Social Security Administration Data" means disclosures of records, information, or data made by the Social Security Administration to HHSC for its administration of federally funded benefit programs under various provisions of the Social Security Act, such as Section 1137 (42 U.S.C. §§ 1320b-7), including the state-funded state supplementary payment programs under Title XVI of the Act, in accordance with the requirements of the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a.

"**Subcontractor**" means a Person or who is not the Workforce of a Business Associate to whom a Business Associate delegates a function, activity or services conducted on behalf of HHSC, as more fully described in HIPAA Regulations.

"Texas Breach Law" means the Texas Identity Theft Enforcement and Protection Act, Texas Business & Commerce Code Ch. 521 and Texas Government Code §2054.1125.

"Unsecured Protected Health Information" means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized Persons through the use of a technology or methodology specified by the Secretary in HITECH Act regulations and HIPAA Security Regulations. Unsecured Protected Health Information does not include:

(1) Encrypted Electronic Protected Health Information; or

(2) Destruction of the media on which the PHI is stored.

All terms used in this DUA that are not otherwise defined in this DUA have the same meaning as those terms in HIPAA or other applicable law relating to CONTRACTOR's use or disclosure of Confidential Information on behalf of HHSC.

"**Workforce**" means employees, volunteers, trainees, and other Persons whose conduct, in the performance of work for HHSC, is under the direct control of HHSC, whether or not they are paid by HHSC.

ARTICLE 3. DATA USE TERMS AND CONDITIONS

The Data Use Terms and Conditions are described in attachments to this DUA and are incorporated by reference. Requirements to create, receive, maintain, use, disclose, have access to or transmit Confidential Information are described in Attachment 1. The Scope of Work is described in Attachment 2. Other Obligations of CONTRACTOR are described in Attachment 3. CONTRACTOR obligations regarding disposition of Confidential Information are described in Attachment 4. General provisions related to this DUA are described in Attachment 5. A description of Confidential Information related to this DUA is provided in Attachment 6. Information Security Guidelines and Procedures are described in Attachment 7. The List of CONTRACTOR's Authorized Users under this DUA is provided in Attachment 8. The Form Subcontractor Agreement is provided in Attachment 9.

ARTICLE 4. AUTHORITY TO EXECUTE

The Parties have executed this DUA in their capacities as stated below with authority to bind their organizations on the dates set forth by their signatures.

IN WITNESS HEREOF, HHSC and CONTRACTOR have each caused this DUA to be signed and delivered by its duly authorized representative:

HEALTH AND HUMAN SERVICES COMMISSION	**CONTRACTOR**
BY: _____	**BY:** _____
NAME: KAY GHAHREMANI	**NAME:** James K Wilson
TITLE: ASSOCIATE COMMISSIONER FOR MEDICAID CHIP DIVISION	**TITLE:** Superintendent
DATE: _____, 201____	**DATE:** 11/11, 2014

ATTACHMENT 1. ACCESS, USE, DISCLOSURE OF CONFIDENTIAL INFORMATION

Section A1.01 ***Ownership of Confidential Information***

CONTRACTOR acknowledges and agrees that the Confidential Information is and will remain the property of HHSC. CONTRACTOR agrees it acquires no title or rights to the Confidential Information, including without limitation, PHI, Limited Data Sets and/or De-identified information, as a result of this DUA.

Section A1.02 ***General Obligations of CONTRACTOR***

CONTRACTOR acknowledges and agrees that it may create, receive, maintain, use, disclose, have access to or transmit Confidential Information only for an Authorized Purpose, and that it may not disclose any Confidential Information to a third party except as may be expressly authorized under this DUA or as Required by Law. HHSC will allow CONTRACTOR to create, receive, maintain, use, disclose, have access to or transmit Confidential Information for an Authorized Purpose, provided CONTRACTOR complies in all respects with the terms and conditions of this DUA and law applicable to the Confidential Information.

Section A1.03 ***Specific Duties and Obligations of CONTRACTOR***

(1) CONTRACTOR agrees, in consideration of HHSC's allowing CONTRACTOR to create, receive, maintain, use, disclose, have access to or transmit Confidential Information, that:

(A) CONTRACTOR will hold the Confidential Information in trust and in strictest confidence;

(B) CONTRACTOR will take all measures necessary to prevent any portion of the Confidential Information from:

(i) Being used in a manner that is not expressly an Authorized Purpose under this DUA or as Required by Law;

(ii) Falling into the public domain; or

(iii) Falling into the possession of Persons not bound to maintain the confidentiality of the Confidential Information.

(C) The minimum measures taken by CONTRACTOR pursuant to this Section include the exercise of reasonable care and at least the same degree of care as CONTRACTOR protects its own confidential, proprietary and trade secret information.

(D) CONTRACTOR will not, without HHSC's prior written consent, disclose or allow access to any portion of the Confidential Information to any Person or other entity, other than Authorized User employees or Subcontractors of CONTRACTOR.

(E) CONTRACTOR will, where provided, comply with the applicable provisions of HIPAA and other law applicable to Confidential Information relating to CONTRACTOR's creation, receipt, maintenance, use, disclosure, access to or transmission of Confidential Information on behalf of HHSC.

(2) CONTRACTOR will have the limited right to create, receive, maintain, use, disclose, have access to or transmit the Confidential Information solely and exclusively for an Authorized Purpose, provided that such would not violate HIPAA or other applicable law relating to Confidential Information if such use or disclosure had been made by HHSC.

(3) CONTRACTOR will allow access to or disclose Confidential Information only to those Subcontractors or Workforce who are Authorized Users trained in data privacy and security and who have a reasonable and demonstrable need to create, receive, maintain, use, disclose, have access to or transmit the Confidential Information to carry out CONTRACTOR's obligations in connection with the Authorized Purpose.

(4) CONTRACTOR will establish, implement and maintain appropriate sanctions against any Workforce or Subcontractor who fails to comply with an Authorized Purpose in violation of this DUA, the Base Contract or applicable law.

(5) CONTRACTOR will not, without prior written approval of HHSC, disclose or provide access to any Confidential Information on the basis that such act is Required by Law without notifying HHSC so that HHSC may have the opportunity to object to the disclosure or access and seek appropriate relief. If HHSC objects to such disclosure or access, CONTRACTOR will refrain from disclosing or providing access to the Confidential Information until HHSC has exhausted all alternatives for relief. Such disclosures of PHI are also addressed in Section 3.04(3), below.

(6) CONTRACTOR will limit creation, receipt, maintenance, use, disclosure, access to or transmission of Confidential Information to the minimum necessary to accomplish an Authorized Purpose.

(7) 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 HHSC or as expressly permitted by the Base Contract.

(8) CONTRACTOR will not permit or enter into any agreement with a Subcontractor to create, receive, maintain, use, disclose, have access to or transmit Confidential Information, on behalf of CONTRACTOR without express written approval of HHSC, in advance. HHSC prior approval, at a minimum will require that:

(A) Subcontractor and CONTRACTOR execute the Form Subcontractor Agreement, Attachment 9, which ensures the subcontract contains identical terms, conditions, safeguards and restrictions as contained in this DUA for PHI and any other relevant Confidential Information and which permits more strict limitations;

(B) The Subcontractor is approved by HHSC through the official Base Contract correspondence process; and

(C) HHSC will be a third-party beneficiary to any agreement between the CONTRACTOR and a Subcontractor or third-party related to the Confidential Information, and HHSC will have the right but not the obligation to enforce the terms of any such agreement directly against the Subcontractor or third party.

(9) The obligations of CONTRACTOR under this section are in addition to the duties of CONTRACTOR with respect to Confidential Information described elsewhere in the DUA, the Base Contract or applicable law.

Section A1.04 ***Other Permissible Uses and Disclosures of PHI by CONTRACTOR***

Except as otherwise limited by this DUA, the Base Contract or law applicable to the Confidential Information, CONTRACTOR, as a HIPAA Business Associate of HHSC,, without limiting other requirements applicable to HHSC Confidential Information, such as PHI, may:

(1) Create, receive, maintain, use, disclose, have access to or transmit PHI to perform the Services and Deliverables of the Base Contract, provided that such:

(A) is not a violation of HIPAA if done by HHSC;

(B) is limited to the minimum necessary to accomplish Authorized Purposes; and

(C) is done in compliance with applicable privacy and security standards for the Confidential Information.

(2) *Use* PHI for the proper management and administration of CONTRACTOR or to carry out CONTRACTOR's legal responsibilities.

(3) *Disclose* PHI for the proper management and administration of CONTRACTOR or to carry out CONTRACTOR's legal responsibilities if:

(A) Disclosure is Required by Law, provided CONTRACTOR complies with Section A1.03(5);

(B) CONTRACTOR obtains reasonable assurances from the Person to whom the information is disclosed that the Person will:

(i) Maintain the confidentiality of the Confidential Information;

(ii) Only 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

(iii) Notify CONTRACTOR of any Event or Breach of Confidential Information of which the Person discovers or should have discovered with the exercise of reasonable diligence, as described in Section A1.06.

(4) Use PHI to provide data aggregation services to HHSC, as that term is defined in the HIPAA, 45 C.F.R. §164.501 and permitted by 45 C.F.R. §164.504(e)(2)(i)(B) and other applicable provisions of HIPAA.

Section A1.05 ***Security Requirements for Confidential Information***

(1) **Secure creation, maintenance, use, disclosure or transmission.** CONTRACTOR will create, maintain, use, disclose, transmit or destroy Confidential Information in a secure fashion. CONTRACTOR must:

(A) Ensure the confidentiality, integrity, and availability of all Confidential Information including without limitation electronic PHI that CONTRACTOR creates, receives, maintains, or transmits;

(B) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

(C) Protect against any reasonably anticipated uses or disclosures of such information that are unauthorized;

(D) Ensure security compliance by training or and sanctions for violations against CONTRACTOR'S Workforce; and

(E) Review and modify the security measures implemented as needed to continue provision of reasonable and appropriate protection of Confidential Information, and update documentation of such security measures.

(2) **Safeguards.** CONTRACTOR will establish, implement and maintain any and all appropriate procedural, administrative, physical and technical safeguards to preserve and

maintain the confidentiality, integrity, and availability of the Confidential Information, and with respect to PHI, as described in the HIPAA Privacy and Security Regulations, or other applicable laws or regulations relating to Confidential Information, to prevent any unauthorized use or disclosure of Confidential Information as long as CONTRACTOR has such Confidential Information in its actual or constructive possession.

(3) **Security Program.** CONTRACTOR will establish, implement and maintain an ongoing security program for Confidential Information, including without limitation for PHI in compliance with the HIPAA Security Regulations that must:

(A) Address administrative, physical, and technical safeguards that reasonably and appropriately protects the confidentiality, integrity, and availability of the Confidential Information, including without limitation PHI, that it creates, receives, maintains, or transmits on behalf of HHSC as in specified.

(B) Address systems of risk assessment and periodic assessments, risk management security measures and information system activity risk reviews.

(C) Designate and identify two Persons, as 1) Chief Privacy Officer and 2) Chief Information Security Officer, each of whom are considered Key Personnel in the Base Contract subject to HHSC approval or rejection, responsible for the development and implementation of the privacy and security requirements in this DUA.

(D) Require Workforce training and sanctions for any CONTRACTOR Director, Officer, Workforce, employee, Subcontractor, or agent who violates the requirements regarding Confidential Information in this DUA, the Base Contract, or laws or regulations applicable to the Confidential Information.

(E) Implement, update as necessary and document reasonable and appropriate policies and procedures to comply with the privacy and security requirements of this DUA.

(F) Implement update as necessary and document policies, procedures, and an Incident Response Plan, in advance of conducting work under the DUA, for mitigating, to the maximum extent practicable, any harmful effect of an unauthorized use or disclosure of Confidential Information or a breach, including without limitation, PHI.

(4) **Security Policies and Procedures Production and Approval.** CONTRACTOR will produce copies of its information security and privacy policies and procedures for HHSC's review and approval upon request by HHSC the following business day or other agreed upon time frame, and make available to the Secretary, in a time and manner reasonably agreed upon or designated by the Secretary, for purposes of the Secretary determining HHSC's or CONTRACTOR's compliance with HIPAA.

(5) **Method of Confidential Information Access or Transfer.** All transmissions of Confidential Information by CONTRACTOR will be conducted securely. Secure transmissions of electronic Confidential Information *in motion* include secure File Transfer Protocol (SFTP) or Encryption at an appropriate level or otherwise protected as required by rule, regulation or law. Secure transmissions of electronic HHSC Confidential Information *at rest* requires Encryption unless there is adequate administrative, technical, and physical security, or as otherwise protected as required by rule, regulation or law. All electronic data transfer and communications of Confidential Information will be through secure systems. Proof of system, media or device security and/or Encryption must be produced to HHSC no later than 48 hours after HHSC's written request in response to the Discovery of an Event or Breach. Otherwise, requested production of such proof will be made as agreed upon by the parties. Redaction is

specifically excluded as a means to ensure security. De-identification of HHSC 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.

(6) **Information Security Guidelines and Procedures.** CONTRACTOR will comply with the requirements and guidelines identified in Attachment 7 of this DUA to ensure the security and confidentiality of the Confidential Information.

Section A1.06 ***Breach Notification, Report and Mitigation Requirements***

(1) Breach or Event Notification to HHSC.

(A) Because HHSC is subject to one-hour reporting under Internal Revenue Services, Social Security Administration and CMS Medicaid requirements, CONTRACTOR will immediately, within the first, consecutive clock hour, or in a timeframe otherwise approved by HHSC in writing, initially report to HHSC's Privacy and Security Officers via email at: privacy@hhsc.state.tx.us, and report as required by the Base Contract all available information about the Discovery of an Event or a Breach of the privacy or security of Confidential Information which is not in compliance with the terms of the DUA, the Base Contract or other laws applicable to Confidential Information.

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

(C) 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 HHSC's satisfaction.

(D) No later than 48 consecutive clock hours after Discovery, or a time within Discovery reasonably should have been made of an Event or Breach of Confidential Information, or within a timeframe otherwise approved by HHSC in writing, provide formal notification to the State. Such notice will include all reasonably available information about the Event or Breach, including without limitation and to the extent available:

1) The date the Event or Breach occurred;

2) The date of CONTRACTOR's and if applicable Subcontractor's Discovery;

3) A brief description of the Event or Breach;

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

5) 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;

6) CONTRACTOR's initial Risk Assessment of the Event or Breach required by applicable law or this DUA for HHSC approval;

7) CONTRACTOR's recommendation for HHSC'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;

8) Contact procedures for Individual to ask questions or learn additional information, including the name and title of a CONTRACTOR representative and a toll free telephone number, an e-mail address and website or postal address;

9) The status of CONTRACTOR's investigation;

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

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

12) A description of how the Event or Breach occurred, who is responsible for the occurrence, or estimations thereof;

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

14) Name a single point of contact and a back-up for CONTRACTOR, with applicable full contact information for both on and off business hours for HHSC to communicate with during the incident response;

15) A reasonable schedule for CONTRACTOR to provide regular updates to the foregoing in the future, as directed by and approved by HHSC for response to the Event or Breach, but no less than every three (3) business days or as otherwise directed by HHSC, including estimation date investigation, reporting, if any, notification, if any, mitigation and root cause analysis is expected to be completed; and

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

(2) Investigation, Response and Mitigation.

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

(B) CONTRACTOR will have implemented policies, procedures and processes to respond to an Event or Breach, prior to start of work under the Base Contract, including investigation, response, root cause analysis, notifications, reporting and mitigation to the maximum extent practicable, any harmful effect of unauthorized use or disclosure of Confidential Information.

(C) CONTRACTOR will update as necessary, policies, procedures and processes to detect, investigate, mitigate losses, and prevent or reduce the likelihood of recurrence of a similar Event or Breach, and to provide these to HHSC for review and approval of the policies, procedures, processes, and the specific findings and actions taken in the time and manner reasonably requested by HHSC.

(D) CONTRACTOR will complete or participate in a Risk Assessment as directed by HHSC following an Event or Breach, and provide the final assessment and mitigations to HHSC for review and approval.

(E) CONTRACTOR will fully cooperate with HHSC to respond to inquiries and/or proceedings by state and federal authorities, Persons and/or Individuals.

(F) CONTRACTOR will fully cooperate with HHSC'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 HHSC in a Corrective Action Plan if directed by HHSC under Article 11 of the Base Contract.

(3) Breach Notification to Individuals and Reporting to Authorities.

(A) Whether legally required or not, HHSC may direct CONTRACTOR to provide breach notification to Individuals, regulators or third-parties, as specified by HHSC following a breach.

(B) CONTRACTOR must obtain HHSC's prior written approval of the time, manner and content of any notification to Individuals, regulators or third-parties, or any notice required by other state or federal authorities. CONTRACTOR will provide HHSC with copies of distributed and approved communications.

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

(D) If HHSC delegates such requirements to Contractor, HHSC 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.

(4) **Training and Education.** CONTRACTOR will ensure its officers, directors, employees, agents, Subcontractors and Workforce are adequately trained and educated and annually refresher or retrained on confidentiality, privacy, security and the importance of promptly reporting any Event or Breach and of the consequences of failing to do so, including without limitation: employment disciplinary action, employer sanctions or enforcement actions for legal noncompliance, potential loss of HHSC's Federal Financial Participation, and risks to third-party agreements. HHSC, at its election, may assist CONTRACTOR in training and education on specific or unique HHSC processes, systems and/or requirements.

ATTACHMENT 2. SCOPE OF WORK

The Scope of Work is set forth in detail in Section I. Medicaid Administration of the Base Contract, HHSC Contract No._____, as amended, between HHSC and CONTRACTOR and is incorporated by reference as if set out word-for-word in this document.

ATTACHMENT 3. OTHER OBLIGATIONS OF CONTRACTOR

Section A3.01 ***Location of Confidential Information; Custodial Responsibility***

CONTRACTOR is designated as the custodian of the records to which it may be entrusted and that contain Confidential Information, and is responsible for compliance with and enforcement of all conditions for creation, maintenance, use, disclosure, transmission and destruction of confidentiality, privacy and Subcontractor agreements as specified in this DUA or as may be reasonably necessary to prevent unauthorized use. CONTRACTOR will store all Confidential Information in a secure area and, subject to the terms of this DUA, will destroy any paper material in a secure manner in accordance with the requirements of the Information Security Guidelines and Procedures in Attachment 7 and Disposition of Confidential Information in Attachment 4.

Section A3.02 ***PHI in Designated Record Set***

(1) CONTRACTOR will make PHI in a Designated Record Set available to HHSC or, as directed by HHSC, provide PHI to the Individual, or legally authorized representative of the Individual, in compliance with the requirements of the HIPAA Privacy Regulations, and make other Confidential Information in CONTRACTOR's possession available pursuant to the requirements of the HIPAA in case of a need for notification by HHSC upon a determination of a Breach of Unsecured PHI as defined in HIPAA.

(2) CONTRACTOR will make PHI in a Designated Record Set available to HHSC for amendment and incorporate any amendments to this information that HHSC directs or agrees to pursuant to the HIPAA.

Section A3.03 ***CONTRACTOR Recordkeeping, Accounting and Disclosure Tracking***

(1) **Accounting, Access or Amendment**. Contractor will document and make available to HHSC the PHI required to provide access, an accounting of disclosures or amendment in compliance with the requirements of the HIPAA Privacy Regulations.

(2) If CONTRACTOR receives a request for access, amendment or accounting of PHI by any Individual subject to this DUA, it will promptly forward the request to HHSC; however, if it would violate HIPAA to forward the request, CONTRACTOR will promptly notify HHSC of the request and of CONTRACTOR's response. Unless CONTRACTOR is prohibited by law from forwarding a request, HHSC will respond to all such requests.

(3) **DHHS Inspection.** Make internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by the CONTRACTOR on behalf of HHSC, available to the Secretary of the U.S. Department of Health and Human Services or the Secretary's designee for purposes of determining compliance with HIPAA.

(4) **Compliance Certification.** CONTRACTOR will provide, and will cause its Subcontractors and agents to provide, to HHSC 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, including without limitation, PHI, EPHI, Unsecured PHI and PII. Written evidence of compliance must be acceptable to HHSC in its sole discretion. Such evidence may include but is not necessarily limited to the following:

(A) Statement on Standards for Attestation Engagements (SSAE) No. 16,, Reporting on Controls at a Service Organization, issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in April 2010.

(B) General security controls audit conducted in accordance with generally-accepted industry standards by a qualified and independent auditor that is acceptable to HHSC;

(C) Application controls audit conducted in accordance with generally-accepted industry standards by a qualified and independent auditor that is acceptable to HHSC;

(D) Vulnerability assessment conducted in accordance with generally-accepted industry standards by a qualified and independent expert in telecommunications and information security that is acceptable to HHSC;

(E) Network/systems penetration test conducted in accordance with generally-accepted industry standards by a qualified and independent expert in telecommunications and information security that is acceptable to HHSC; and

(F) Risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI subject to this DUA.

ATTACHMENT 4. DISPOSITION OF CONFIDENTIAL INFORMATION

Section A4.01 ***CONTRACTOR's Duty in General***

CONTRACTOR will return, destroy, or continue to maintain appropriate safeguards for Confidential Information, including without limitation all PHI received from HHSC or created, received or maintained on behalf of HHSC, as directed by HHSC, upon termination of the DUA or Base Contract.

Section A4.02 ***Return or Destruction of Confidential Information***

(1) CONTRACTOR agrees that on the termination or expiration of this DUA, CONTRACTOR will, at its expense, return to HHSC or destroy, at HHSC's election, and to the extent reasonably feasible and permissible by law, all Confidential Information received from HHSC or created or maintained by CONTRACTOR or any of CONTRACTOR's agents or Subcontractors on HHSC's behalf if that data contains Confidential Information. CONTRACTOR will certify in writing to HHSC that all the Confidential Information that has been created, received, maintained, used by or disclosed to CONTRACTOR, has been destroyed or returned to HHSC, and that CONTRACTOR and its agents and Subcontractors have retained no copies thereof. Notwithstanding the foregoing, CONTRACTOR acknowledges and agrees that it may not destroy any Confidential Information if federal or state law prohibits such destruction.

(2) If such return or destruction is not reasonably feasible, or is impermissible by law, immediately notify HHSC of the reasons such return or destruction is not feasible, and agree to extend indefinitely the protections of this DUA to the Confidential Information and limit its further uses and disclosures to the purposes that make the return of the Confidential Information not feasible for as long as CONTRACTOR maintains such Confidential Information.

ATTACHMENT 5. GENERAL PROVISIONS

Section A5.01 ***HHSC commitment and obligations***

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

Section A5.02 ***HHSC Right to Inspection***

At any time upon reasonable notice to CONTRACTOR, or if HHSC determines that CONTRACTOR has violated this DUA, HHSC, 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, HHSC's agent(s) include, without limitation, the HHSC Office of the Inspector General or the Office of the Attorney General of Texas or other designee. HHSC's failure to inspect or failure to detect any noncompliance with the DUA or through its agent's inspection does not relieve CONTRACTOR of its responsibility to comply with this DUA.

Section A5.03 ***Access to PHI***

CONTRACTOR will make available to HHSC any information HHSC requires to fulfill HHSC's obligations to provide access to, and copies of, PHI in accordance with HIPAA and other applicable laws and regulations of Confidential Information.

Section A5.04 ***Term of DUA***

This DUA will be effective on the date on which CONTRACTOR executes the DUA, and will expire on the date specified in the DUA.

(1) Either party may terminate this DUA at any time upon 30 days written notice to the other party.

(2) HHSC may immediately terminate this DUA on:

(A) A material violation of this DUA. "Material" means:

(i) any violation by CONTRACTOR of a material term of this DUA will be considered a breach of contract if the CONTRACTOR knew of or reasonably should have known of the violation and failed to immediately take reasonable steps to cure it and notify HHSC, as required by the DUA;

(ii) CONTRACTOR fails to timely notify HHSC of an Event or Breach, or take corrective action required;

(iii) CONTRACTOR's repeated or flagrant violation of the obligations under the DUA;

(iv) CONTRACTOR's failure to respond to a demand letter concerning penalties under the DUA or Base Contract;

(v) CONTRACTOR being named as a defendant in a criminal proceeding for a violation of HIPAA, or other applicable laws and regulations of Confidential Information; and/or

(vi) a finding or stipulation that CONTRACTOR has violated any standard or requirement of HIPAA other laws and regulations of Confidential

Information; or other security or privacy law in an administrative or civil proceeding which CONTRACTOR has been joined.

(vii) If neither termination nor cure is feasible, HHSC shall report the violation to the Secretary.

(3) Termination of this DUA will not relieve CONTRACTOR of its duties with regards to the return or disposition of the Confidential Information as set forth in this DUA.

(4) **Termination Options.** If HHSC determines that CONTRACTOR has violated a material term of this DUA; HHSC may in its sole discretion:

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

(B) Require CONTRACTOR to submit to a Corrective Action Plan under Article 14 of the Base Contract, plan for monitoring and plan for reporting, as HHSC may determine necessary to maintain compliance with this DUA; and/or

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

(ii) Terminate the DUA and Base Contract immediately, and seek relief in a court of competent jurisdiction in Travis County, Texas; and

(iii) Before exercising any of these options, HHSC will provide written notice to CONTRACTOR describing the violation and the action it intends to take.

Section A5.05 ***Publication***

CONTRACTOR may not publish or otherwise disclose to a third party any results of work under the DUA or Base Contract unless HHSC expressly approved in writing of such disclosure in advance of such publication.

Section A5.06 ***Governing Law, Venue and Litigation***

(1) 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.

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

Section A5.07 ***Injunctive Relief***

(1) CONTRACTOR understands and agrees that HHSC 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.

(2) CONTRACTOR further agrees that monetary damages may be inadequate to compensate HHSC for CONTRACTOR's or its Subcontractor's failure to comply. Accordingly, CONTRACTOR agrees that HHSC 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.

(3) The duties of CONTRACTOR or its Subcontractor under this DUA survive the expiration of this DUA until all the Confidential Information is destroyed or returned to HHSC, as required by this DUA.

Section A5.08 ***Indemnification***

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

Section A5.09 ***Insurance***

(1) In addition to any insurance required in the Base Contract, at HHSC's option and as directed, HHSC may require CONTRACTOR to maintain, at its expense, the following special and/or custom first- and third-party insurance coverages, naming the State of Texas, acting through HHSC, as an additional named insured and loss payee, with primary and non-contributory status, with required insurance coverage, by the Effective Date of the request, or as required by HHSC:

(A) Network Security and Privacy;

(B) Data Breach;

(C) 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);

(D) Electronic Media Liability;

(E) Crime/Theft;

(F) Advertising Injury and Personal Injury Liability; and

(G) Crisis Management and Notification Expense Coverage.

(2) CONTRACTOR will provide HHSC with proof of policy part (as opposed to merely a certificate of coverage or binder), at the request of HHSC.

Section A5.10 ***Fees and Costs***

Except as otherwise specified in this DUA or the Base Contract, including but not limited to requirements to insure and/or indemnify HHSC, if any legal action or other proceeding is brought for the enforcement of this DUA, or because of an alleged dispute, contract violation, Event, Breach, default,

misrepresentation, or injunctive action, in connection with any of the provisions of this DUA, each party will bear their own legal expenses and the other cost incurred in that action or proceeding.

Section A5.11 ***Entirety of the Base Contract***

The Base Contract consists of this Business Associate Agreement and the Base Contract and constitutes the entire agreement between the parties. There are no understandings or agreements relating to this DUA or the Base Contract that are not fully expressed therein and 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. To the extent of any conflicts exist between this DUA and the Base Contract, this DUA controls.

Section A5.12 ***Automatic Amendment and Interpretation***

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

ATTACHMENT 6. CONFIDENTIAL INFORMATION

Any information under the terms of the Base Contract, HHSC Contract No. _____ between HHSC and CONTRACTOR, as amended, that HHSC may provide or make available to CONTRACTOR, or that CONTRACTOR may create, receive, maintain or have access to on behalf of HHSC that is defined as Confidential above.

ATTACHMENT 7. SECURITY GUIDELINES AND PROCEDURES

CONTRACTOR and all Subcontractors, consultants, or agents under the DUA (collectively "CONTRACTOR") must comply at a minimum with the following **Information Security Guidelines and Procedures** currently in effect:

- HHS Circular C-021, *Health and Human Services Enterprise Information Security Standards and Guidelines*;
- HHS Enterprise Information Security Standards and Guidelines (EISSG);
- HHS Enterprise Information Security Controls Catalog (EISSC); and
- Title 1, Sections 202.1 and 202.3, and Subchapter B, Texas Administrative Code.

CONTRACTOR must comply with at least the following, *as applicable*:

- 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 Publication 800-53 – Recommended Security Controls for Federal Information Systems and Organizations, as currently revised;
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems; and
- NIST Special Publication 800-88, Guidelines for Media Sanitization

In addition to the requirements expressly stated in this Section, CONTRACTOR must comply with any other State or Federal law, regulation, or administrative rule relating to the specific HHSC program area that CONTRACTOR supports on behalf of HHSC.

ATTACHMENT 8. LIST OF AUTHORIZED USERS

CONTRACTOR represents and warrants that each of those Workforce below have a demonstrated need to know and have access to Confidential Information pursuant to this DUA and the Base Contract, and further, that each agree to be bound by the disclosure and use limitations pertaining to the Confidential Information contained in the DUA. CONTRACTOR must maintain an updated, complete, accurate and numbered list of Authorized Users at all times and supply it to HHSC, as directed, to the extent those identified below change:

1. Signature: _____
   Name: Debbie Roybal
   Title: Executive Director Special Education
   Date: 11/7/14

2. Signature: _____
   Name: Bob Gorton
   Title: Sp Ed Related Services Supervisor
   Date: 11/7/14

3. Signature: _____
   Name: Debbie Monschke
   Title: Assistant Superintendent Administrative Services
   Date: 11/7/14

4. Signature: _____
   Name: Cathi Robbins
   Title: Grants Accountant
   Date: 11/7/14

5. Signature: _____
   Name: Melissa Aleman
   Title: Accounts Payable Supervisor
   Date: 11/7/14

6. Signature: _____
   Name: Julie Simpson
   Title: Accounting Supervisor
   Date: 11/7/14

7. Signature: _____
   Name: James K Wilson
   Title: Superintendent
   Date: 11/7/14

8. Signature: _____
   Name: _____
   Title: _____
   Date: _____

9. Signature: _____
   Name: _____
   Title: _____
   Date: _____

10. Signature: _____
    Name: _____
    Title: _____
    Date: _____

11. Signature: _____
Name: _____
Title: _____
Date: _____

12. Signature: _____
Name: _____
Title: _____
Date: _____

13. Signature: _____
Name: _____
Title: _____
Date: _____

14. Signature: _____
Name: _____
Title: _____
Date: _____

15. Signature: _____
Name: _____
Title: _____
Date: _____

16. Signature: _____
Name: _____
Title: _____
Date: _____

17. Signature: _____
Name: _____
Title: _____
Date: _____

18. Signature: _____
Name: _____
Title: _____
Date: _____

19. Signature: _____
Name: _____
Title: _____
Date: _____

20. Signature: _____
Name: _____
Title: _____
Date: _____

21. Signature: _____
Name: _____
Title: _____
Date: _____

22. Signature: _____
Name: _____
Title: _____
Date: _____

23. Signature: _____
Name: _____
Title: _____
Date: _____

24. Signature: _____
Name: _____
Title: _____
Date: _____

25. Signature: _____
Name: _____
Title: _____
Date: _____

26. Signature: _____
Name: _____
Title: _____
Date: _____

27. Signature: _____
Name: _____
Title: _____
Date: _____

28. Signature: _____
Name: _____
Title: _____
Date: _____

29. Signature: _____
Name: _____
Title: _____
Date: _____

30. Signature: _____
Name: _____
Title: _____
Date: _____

31. Signature: _____
Name: _____
Title: _____
Date: _____

32. Signature: _____
Name: _____
Title: _____
Date: _____

33. Signature: _____
Name: _____
Title: _____
Date: _____

34. Signature: _____
Name: _____
Title: _____
Date: _____

35. Signature: _____
Name: _____
Title: _____
Date: _____

36. Signature: _____
Name: _____
Title: _____
Date: _____

ATTACHMENT 9. SUBCONTRACTOR AGREEMENT FORM

The DUA between HHSC and CONTRACTOR establishes the permitted and required uses and disclosures of Confidential Information by CONTRACTOR.

CONTRACTOR has subcontracted with_____ (SUBCONTRACTOR) for performance of duties on behalf of CONTACTOR which are subject to the DUA [describe SUBCONTRACTOR's duties which fall under the terms and conditions of the DUA or attach a Scope of Work or Subcontract and incorporate it by reference in this Form]: _____.

SUBCONTRACTOR acknowledges, understands and agrees to be bound by the terms and conditions applicable to CONTRACTOR under the DUA, incorporated by reference in this Agreement, with respect to HHSC Confidential Information. CONTRACTOR and SUBCONTRACTOR assure HHSC that SUBCONTRACTOR will only create, receive, maintain, or transmit Confidential Information on behalf of CONTRACTOR under , *at a minimum,* the identical terms and conditions of the DUA applicable to CONTRACTOR. The DUA represents minimum requirements over HHSC Confidential Information. CONTRACTOR may apply stricter requirements over HHSC Confidential Information to SUBCONTRACTOR than apply to CONTRACTOR in the DUA CONTRACTOR may also contract with SUBCONTRACTOR to engage in activities not subject to the DUA, if not prohibited by the Base Contract.

SUBCONTRACTOR acknowledges receipt, understanding of and agrees to be bound by the terms and conditions applicable to SUBCONTRACTOR under the DUA with respect to HHSC Confidential Information, which is incorporated by reference for purposes of SUBCONTRACTOR's agreement as if fully set forth herein.

CONTRACTOR and SUBCONTRACTOR agree that HHSC is a third-party beneficiary to applicable provisions of the subcontract.

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

CONTRACTOR and SUBCONTRACTOR assure HHSC that any Breach or Event as defined by the DUA that SUBCONTRACTOR discovers will be reported to HHSC by CONTRACTOR in the time, manner and content required by the DUA.

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

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

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

CONTRACTOR

BY:_____

NAME:_____

TITLE: _____

DATE _____, 201_____

SUBCONTRACTOR

BY:_____

NAME:_____

TITLE: _____

DATE _____, 201_____