

MAC Business Associate Agreement

Please complete the following steps:

- 1) Print the Business Associate Agreement and obtain original signatures.
- 2) Please fill in your entity's information in the appropriate fields. Your entity's name serves as the "contractor". The Business Associate Agreement must be signed by an employee with legal/signature authority.
- 3) Please leave the "HHSC Contract No." fields blanks as the contract's department will assign a contract number (HCAT number) once the contract has been fully executed.
- 4) Attachment 8 – The entity is required to identify users who have access to confidential data as it relates Medicaid Administrative activities performed under the Intergovernmental Cooperation Agreement. The entity is to maintain the list of authorized users and is required to supply that information upon request from HHSC. In the case where voluminous authorized users exists, the list must be maintained by the entity with an obligation to ensure that those given access are aware of and trained on confidentiality requirements. In addition, the list must be updated regularly and modified as appropriate, e.g. when someone leaves employment.
- 5) Mail the signed, original document to HHSC Rate Analysis.
- 6) Photocopies will not be accepted.
- 7) HHSC contract's department will return the executed copy of the agreement to your entity. The agreement will include the entity's contract number (HCAT number).

**DATA USE AND BUSINESS ASSOCIATE AGREEMENT
BETWEEN HEALTH AND HUMAN SERVICES COMMISSION
AND**

_____ (“CONTRACTOR”)

ARTICLE 1.	PURPOSE.....	2
ARTICLE 2.	DEFINITIONS.....	2
Section 2.01	Definition of Confidential Information.....	2
Section 2.02	Other Definitions	3
ARTICLE 3.	Data Use Terms and Conditions	8
ARTICLE 4.	Authority To Execute.....	8
ATTACHMENT 1.	Access, Use, Disclosure of Confidential Information	1
Section A1.01	Ownership of Confidential Information.....	1
Section A1.02	General Obligations of CONTRACTOR.....	1
Section A1.03	Specific Duties and Obligations of CONTRACTOR.....	1
Section A1.04	Other Permissible Uses and Disclosures of PHI by CONTRACTOR.....	2
Section A1.05	Security Requirements for Confidential Information	3
Section A1.06	Breach Notification, Report and Mitigation Requirements	4
ATTACHMENT 2.	Scope of Work	1
ATTACHMENT 3.	Other Obligations of CONTRACTOR	1
Section A3.01	Location of Confidential Information; Custodial Responsibility	1
Section A3.02	PHI in Designated Record Set	1
Section A3.03	CONTRACTOR Recordkeeping, Accounting and Disclosure Tracking	1
ATTACHMENT 4.	Disposition of Confidential Information.....	1
Section A4.01	CONTRACTOR’s Duty in General.....	1
Section A4.02	Return or Destruction of Confidential Information	1
ATTACHMENT 5.	General Provisions	1
Section A5.01	HHSC commitment and obligations	1
Section A5.02	HHSC Right to Inspection	1
Section A5.03	Access to PHI.....	1
Section A5.04	Term of BAA	1
Section A5.05	Publication	2
Section A5.06	Governing Law, Venue and Litigation	2
Section A5.07	Injunctive Relief.....	2
Section A5.08	Indemnification	3
Section A5.09	Insurance	3
Section A5.10	Fees and Costs.....	3
Section A5.11	Entirety of the Base Contract.....	4
Section A5.12	Automatic Amendment and Interpretation	4
ATTACHMENT 6.	Confidential Information	1
ATTACHMENT 7.	Security Guidelines and Procedures	1
ATTACHMENT 8.	List of Authorized Users	1

STATE OF TEXAS

COUNTY OF TRAVIS

**DATA USE AND BUSINESS ASSOCIATE AGREEMENT
BETWEEN HEALTH AND HUMAN SERVICES COMMISSION
AND**

_____ (“CONTRACTOR”)

This Data Use And Business Associate Agreement (“BAA”), effective as of the date signed below (“Effective Date”), is entered into by and between Health and Human Services Commission (“HHSC”) and _____ (“CONTRACTOR”), and incorporated into the terms of the “Base Contract” entered into by these parties, HHSC Contract No. _____.

ARTICLE 1. PURPOSE

CONTRACTOR requires access to information about HHSC programs and/or its clients for HHSC program benefits and services described in the Base Contract. This information is deemed confidential under 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, availability and appropriate use of the HHSC information.

The purpose of this BAA is to facilitate the sharing of Confidential Information with CONTRACTOR, and clarify CONTRACTOR’s obligations with respect to its access to and use and disclosure of the information. This BAA expressly describes the limited purposes for which the CONTRACTOR may access, use or disclose the information, and establishes CONTRACTOR’s rights and responsibilities concerning the information. This BAA also describes HHSC’s remedies in the event of CONTRACTOR’s noncompliance with its obligations under this BAA.

As of the Effective Date of this BAA, HHSC UNIFORM TERMS AND CONDITIONS, Article 10, Section 16.01 HIPAA, conflicts with this BAA, this BAA controls.

ARTICLE 2. DEFINITIONS

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

Section 2.01 *Definition of Confidential Information*

For the purposes of this BAA, the term “Confidential Information” has the meaning set forth below. Capitalized terms included in this definition 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) Electronic Protected Health Information;
- (3) Federal Tax Information;

- (4) Personally Identifiable Information;
- (5) Protected Health Information;
- (6) Social Security Administration Data;
- (7) Unsecured Protected Health Information;
- (8) All non-public budget, expense, payment and other financial information;
- (9) All privileged work product;
- (10) All information designated as confidential under the laws of the State of Texas and of the United States;
- (11) 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;
- (12) Information that is utilized, developed, received, or maintained by HHSC, the CONTRACTOR, or participating State agencies for the purpose of fulfilling a duty or obligation under this BAA and that has not been publicly disclosed;
- (13) Information identified in Attachment 6 attached to this BAA and to which CONTRACTOR specifically seeks to obtain access for an Authorized Purpose.

Section 2.02 Other Definitions

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

“Authorized Purpose” means the 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 process, view, handle, examine, interpret, or analyze Confidential Information pursuant to this BAA;
- (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 BAA, such agreement evidenced by each Authorized User’s signature on the form attached to this BAA as Attachment 8.

“Breach” means:

- (1) **Breach of PHI.** With respect to Protected Health Information (“PHI”) pursuant to HIPAA and the HITECH Act, including without limitation Electronic Protected Health Information and/or Unsecured Protected Health Information, the acquisition, access, use, or disclosure of PHI in a manner not permitted under this BAA or the Base Contract and/or HIPAA Privacy Regulations or HIPAA Security Regulations, which compromises the security or privacy of the PHI as defined in 45 CFR 164.402.

With respect to PHI, “compromises the security or privacy of the PHI” means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of De-Identified information, date of birth, and zip code does not compromise the security or privacy of the PHI.

With respect to PHI, “breach,” pursuant to HIPAA, 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 HIPAA Privacy Regulations and HIPAA Security Regulations, 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 HHSC or CONTRACTOR has 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 HITECH and the HIPAA Security Regulations.
- (2) **“Breach of System Security,”** as defined by the Texas Breach Law. For purpose of the Texas Breach Law, the currently undefined phrase, “compromises the security, confidentiality, or integrity of sensitive personal information,” will be interpreted in HHSC’s sole discretion, including without limitation, 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, and/or the receipt of satisfactory assurance from the person that the person agrees to further protect and safeguard, return and/or destroy the data subject to the Texas Breach Law to the satisfaction of HHSC; and/or.
- (3) Any unauthorized use or disclosure as defined by any other law and any regulations adopted there under regarding Confidential Information.

“Business Associate” means a person or organization, other than a member of HHSC’s workforce, that performs certain functions or activities on behalf of, or provides certain services to, HHSC that involve the use or disclosure of individually identifiable health information. The meaning of Business Associate is more fully described in the HIPAA Privacy Regulations and HIPAA Security Regulations. CONTRACTOR is a Business Associate of HHSC for purposes of this BAA.

“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” 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 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 as specified in the HIPAA Security Rule Regulations, such that the PHI cannot be retrieved.

“Discovery” means the first day on which an Incident is known to CONTRACTOR, or, by exercising reasonable diligence would have been known to CONTRACTOR, and includes incidents 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 further described in the HIPAA Privacy Regulations and the HIPAA Security Regulations.

“Encrypted Electronic Protected Health Information” means , as specified in 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.

“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, 42 U.S.C. §1320d, et seq., and regulations adopted under that act.

“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. 111-105), and regulations adopted under that act.

“Incident” means a potential 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. An Incident becomes a Breach when the incident involves the suspected or 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.

“Individual” means the subject of the Confidential Information, including without limitation PHI, and will include the subject's legally authorized representative who qualifies under the HIPAA Privacy Regulation as a 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; and Texas Prob. Code § 3:

a 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; and Texas Prob. Code § 3:

- (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 durable power of attorney for health care;
- (4) an attorney ad litem appointed for the Individual;
- (5) a guardian ad litem appointed for the Individual;
- (6) a personal representative or statutory beneficiary if the Individual is deceased;
- (7) an attorney retained by the Individual or by another person listed herein; or
- (8) If an individual is deceased, their personal representative must be the executor, independent executor, administrator, independent administrator, or temporary administrator of the estate.

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

“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, subcontractor, a member of the general public, and/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 patient health information in any form that is created or received by a healthcare provider, and relates to the patient's healthcare condition, provision of healthcare, or payment for the provision of healthcare, as further described and defined in the HIPAA Privacy Regulations. PHI includes demographic information unless such information is De-identified, as defined above. PHI includes without limitation, “Electronic Protected Health Information” as above.

“Required by Law” shall have the same meaning as the term “required by law” in 45 CFR 164.103.

“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 BAA. 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 BAA will be resolved, in HHSC’s sole discretion, by giving effect to the other terms of the Base Contract or this BAA.

“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.

“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 of Health and Human Services under the HITECH Act 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 BAA that are not otherwise defined in this BAA have the same meaning as those terms in HIPAA Privacy Regulations, HIPAA Security Regulations, the HITECH Act, or other applicable law relating to Contractor’s use or disclosure of Confidential Information on behalf of HHSC.

ARTICLE 3. DATA USE TERMS AND CONDITIONS

The Data Use Terms and Conditions are described in attachments to this BAA. Requirements for Access, Use, Disclosure of 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 BAA are described in Attachment 5. A description of Confidential Information related to this BAA is provided in Attachment 6. Information Security Guidelines and Procedures are described in Attachment 7. The List of CONTRACTOR’s Authorized Users under this BAA is provided in Attachment 8.

ARTICLE 4. AUTHORITY TO EXECUTE

The Parties have executed this contract 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 BAA to be signed and delivered by its duly authorized representative:

HEALTH AND HUMAN SERVICES COMMISSION

CONTRACTOR

BY: _____

BY: _____

NAME: Kay Ghahremani

NAME: _____

Associate Commissioner for Medicaid/CHIP
Health and Human Services Commission

TITLE: _____

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 BAA.

Section A1.02 *General Obligations of CONTRACTOR*

CONTRACTOR acknowledges and agrees that it may access and use 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 BAA or as Required by Law. HHSC will allow CONTRACTOR to access the Confidential Information and use and disclose such information for an Authorized Purpose, provided CONTRACTOR complies in all respects with the terms and conditions of this BAA.

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

- (1) CONTRACTOR agrees, in consideration of HHSC's allowing access to 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 BAA 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 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 agents of CONTRACTOR.
 - (E) CONTRACTOR will comply with all applicable requirements of HIPAA, the HIPAA Privacy Regulations, the HIPAA Security Regulations, and the HITECH Act to the extent the Confidential Information contains information that is subject to HIPAA, or other applicable law relating to CONTRACTOR's use and disclosure of Confidential Information on behalf of HHSC.
- (2) CONTRACTOR will have the limited right to access, use and disclose the Confidential Information solely and exclusively for an Authorized Purpose, provided that such use or disclosure would not violate HIPAA, the HIPAA Privacy Regulations, the HIPAA Security

Regulations, the HITECH Act 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 persons who are Authorized Users trained in privacy and data security and who have a reasonable and demonstrable need to access 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 employee, agent or subcontractor who uses or discloses Authorized Purpose in violation of this BAA, the Base Contract or applicable law.
- (5) CONTRACTOR will not, without prior written approval of HHSC, disclose any Confidential Information on the basis that such disclosure is required by law without notifying HHSC so that HHSC may have the opportunity to object to the disclosure and seek appropriate relief. If HHSC objects to such disclosure, CONTRACTOR will refrain from disclosing 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 any use or disclosure to the minimum necessary to accomplish an Authorized Purpose.(7) CONTRACTOR agrees that to the extent that it has access to, receives from HHSC, or creates or receives PHI on behalf of HHSC, CONTRACTOR will fully comply with the requirements of HIPAA, the HIPAA Privacy Regulations, the HIPAA Security Regulations and the HITECH Act with respect to such PHI. To the extent that CONTRACTOR has access to Limited Data Set information, CONTRACTOR agrees to comply with the requirements of HIPAA, the HIPAA Privacy Regulations, the HIPAA Security Regulations and the HITECH Act with respect to such Limited Data Set information;
- (8) CONTRACTOR will not attempt to re-identify or further identify the Confidential Information or De-identified Information, or attempt to contact any Individuals whose records are contained in the Confidential Information, without express written authorization from HHSC or as expressly permitted by the Base Contract.
- (9) CONTRACTOR will not enter into a subcontract for use or disclosure of Confidential Information by any sub-Contractor or agent of CONTRACTOR, without express written approval of HHSC, in advance. HHSC prior approval, at a minimum will require that:
 - (A) The subcontract contains identical terms, conditions, safeguards and restrictions on the use and disclosure of PHI and any other relevant Confidential Information as contained in this BAA;
 - (B) The subcontractor is approved by HHSC;
 - (C) HHSC will be a third party beneficiary to any agreement between the CONTRACTOR and a 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 third party.
- (10) The obligations of CONTRACTOR under this section are in addition to the duties of CONTRACTOR with respect to Confidential Information described elsewhere in the BAA or the Base Contract.

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

Except as otherwise limited by this BAA or the Base Contract, CONTRACTOR may:

- (1) Use or disclose PHI to perform the Services and Deliverables of the Base Contract, as permitted by this BAA, provided that:
 - (A) Such use or disclosure would not violate the HIPAA Privacy Regulations or HIPAA Security Regulations if the use or disclosure were made by HHSC; and
 - (B) Such use or disclosure is limited to the minimum necessary to accomplish the purposes of the use or disclosure.
- (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 will not, without prior written approval of HHSC, disclose any PHI on the basis that such disclosure is Required by Law without notifying HHSC so that HHSC may have the opportunity to object to the disclosure and seek appropriate relief. If HHSC objects to such disclosure, CONTRACTOR will refrain, to the extent possible, from disclosing PHI until HHSC has exhausted all alternatives for relief; or
 - (B) CONTRACTOR obtains reasonable assurances from the Person to whom the information is disclosed that the Person will:
 - (i) Maintain the confidentiality of the PHI;
 - (ii) Use or further disclose the information only as Required by Law or for the purpose for which it was disclosed to the Person; and
 - (iii) Notify CONTRACTOR of any Breach of PHI of which the Person is aware, as described in Section A1.06.
- (4) Use PHI to provide data aggregation services to HHSC, as that term is defined in the HIPAA Privacy Regulations, 45 C.F.R. §164.501 and permitted by 45 C.F.R. §164.504(e)(2)(i)(B) and other applicable provisions of the HIPAA Privacy Regulations.

Section A1.05 Security Requirements for Confidential Information

- (1) **Secure access, use and/or disclosure.** CONTRACTOR will access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose the Confidential Information in a secure fashion. For purposes of this BAA, a secure fashion means that the Confidential Information is rendered unusable, unreadable, or indecipherable to unauthorized persons by either encryption or destruction such that the Confidential Information cannot be read or otherwise reconstructed.
- (2) **Safeguards.** CONTRACTOR will establish, implement and maintain any and all appropriate procedural, physical and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of the Confidential Information, as described in the HIPAA Privacy Regulations, HIPAA Security Regulations, the HITECH Act, 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 compliant with the HIPAA Security Regulations addressing:

- (A) 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 in the HIPAA Security Rule.
 - (B) Systems of risk assessment and periodic assessments, risk management security measures and information system activity risk reviews.
 - (C) Designated Privacy and Security officers, who will be considered Key Personnel in the Base Contract subject to HHSC approval or rejection.
 - (D) Workforce training and sanctions for any CONTRACTOR Director, Officer, workforce member, employee, subcontractor, or agent who violates the requirements regarding Confidential Information in this BAA, the Base Contract, the HIPAA Privacy Regulations, HIPAA Security Regulations, the HITECH Act, and/or law and regulations applicable to the Confidential Information.
 - (C) A System in place for mitigating, to the maximum extent practicable, any harmful effect of a use or disclosure of Confidential Information, including without limitation, PHI other than as provided for by this BAA or applicable law.
- (4) **Security Policies and Procedures.** CONTRACTOR will produce copies of its information security and privacy policies and procedures for HHSC's review and approval upon request by HHSC 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 the HIPAA Privacy or Security Regulations.
- (5) **Method of Confidential Information Access or Transfer.** All transmissions of Confidential Information by CONTRACTOR will be conducted via either a secure File Transfer Protocol site or optical media (e.g., recordable CD or DVD) to be delivered in accordance with HIPAA requirements and HHSC Confidentiality and Security Protocols. All data transfer and communications involving potentially identifying Confidential Information will be through secure systems.
- (6) **Information Security Guidelines and Procedures.** CONTRACTOR will comply with the requirements and guidelines identified in Attachment 7 of this BAA to ensure the security and confidentiality of the Confidential Information.

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

- (1) **Breach Notification to HHSC.**
- (A) CONTRACTOR will immediately, within the first consecutive clock hour, report to HHSC, Discovery of an Incident or a Breach of privacy or security of Confidential Information, including without limitation PHI, Unsecured PHI or EPHI which is not in compliance with the terms of the BAA, the Base Contract or other laws applicable to any Confidential Information.
 - (B) CONTRACTOR will cooperate fully with HHSC in addressing any such unauthorized acquisition, access, use or disclosure, or suspected or potential unauthorized acquisition, access, use or disclosure of Confidential Information including without limitation Unsecured PHI, to the extent and in the manner determined by HHSC.

- (C) CONTRACTOR'S obligation begins at the Discovery of an Incident or Breach and continues as long as related activity continues, until all effects of the incident are mitigated, to HHSC's satisfaction.
- (D) No later than 48 consecutive clock hours after CONTRACTOR discovers or reasonably should have discovered any Incident or Breach of unauthorized acquisition, access, use, or disclosure of Confidential Information, including without limitation Unsecured PHI , provide formal notification to the State. Such notice will include all information to which CONTRACTOR has access, including but not limited to the following information:
 - 1) The date the Incident or Breach of unauthorized acquisition, access, use, or disclosure occurred;
 - 2) The date of Discovery;
 - 3) A brief description of the Incident or Breach of Confidential Information, including without limitation Unsecured PHI, acquired, accessed, used, or disclosed without an Authorized Purpose;
 - 4) A description of the types of Confidential Information involved;
 - 5) Identification and number of all Individuals reasonably believed to be affected, including first and last name of the individual, legally authorized representative, last known address, age, telephone number, email address if preferred contact method, to the extent known or can be reasonably determined by CONTRACTOR;
 - 6) CONTRACTOR's initial assessment of potential harm (i.e.: rating category of low, medium, high level risk) to the Individual or compromise to the information required by the HIPAA Security Regulations or other applicable law (such as the Texas Breach Law), for HHSC approval;
 - 7) 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 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 Individuals 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, 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 another Incident or Breach;
 - 12) A description of how the Incident or Breach occurred and/or estimations thereof;

- 13) A description or estimation of the entities and/or Individuals which may be involved in the Incident or Breach (such as CONTRACTOR, subcontractor, rogue employee, suspected criminal activity and/or law enforcement involvement);
- 14) A single point of contact and a back-up for CONTRACTOR, with applicable full contact information for both on and off business hours;
- 15) A reasonable schedule for CONTRACTOR to provide regular updates to the foregoing, as directed by and approved by HHSC for response to the Incident 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 pertinent information, documents or reports related to an Incident or Breach HHSC requests following Discovery.

(2) Investigation, Response and Mitigation.

- (A) CONTRACTOR will immediately conduct an investigation and respond to the Incident or Breach, and will commit necessary and appropriate staff and resources to expeditiously respond and report to HHSC to ensure HHSC's compliance with report and notification timelines, to the satisfaction of HHSC.
- (B) CONTRACTOR will have procedures and processes to respond to an Incident or Breach, in place prior to the delivery of any Confidential Information, including investigation, incident response, root cause analysis, notification, reporting and mitigation (to the maximum extent practicable, any harmful effect of a use or disclosure of Confidential Information, including without limitation Unsecured PHI, that is contrary to this BAA, the Base Contract, HIPAA, HITECH or other laws applicable to any Confidential Information).
- (C) CONTRACTOR will update as necessary, procedures to investigate the Incident or Breach, mitigate losses, and protect against any future Incident or Breach, and to provide a description of these procedures and the specific findings of the investigation to HHSC in the time and manner reasonably requested by HHSC.
- (D) CONTRACTOR will complete or participate in a risk assessment following an Incident or Breach, and provide the final assessment to HHSC.
- (E) CONTRACTOR will cooperate with HHSC to respond to inquiries and/or proceedings by state and federal authorities and/or Individuals.
- (F) CONTRACTOR will cooperate with HHSC's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such threatened or actual Incident or Breach, or to recover or protect any Confidential Information, including complying with reasonable corrective action or measures, as specified by HHSC and a Corrective Action Plan if directed by HHSC under Article 14 of the Base Contract.

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

- (A) At HHSC's option, CONTRACTOR may be delegated all or part of the requirements to timely notify and report any breach, as specified by HHSC.
- (B) CONTRACTOR must obtain HHSC's prior written approval of the time, manner and content of any notification to Individuals, the media, and/or report as directed by

HHSC to state or federal authorities (regardless of whether or not legally required), and provide HHSC with copies of distributed and approved communications.

- (C) CONTRACTOR will have the burden of demonstrating to the satisfaction of HHSC that all delegated notifications or reports were made as Required by Law; including any evidence demonstrating any delay outside of the control of CONTRACTOR beyond required timelines.
- (4) **Training and Education.** CONTRACTOR will ensure its officers, directors, employees, agents, subcontractors and workforce are adequately trained and educated and periodically retrained on the importance of promptly reporting privacy and security any Incident or Breach and of the consequences of failing to do so, including without limitation, sanctions or enforcement actions for legal noncompliance, potential loss of 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 the Medicaid Administrative Claiming Intergovernmental Cooperation Agreement of the Base Contract, HHSC Contract No. [REDACTED], 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 use, establishment, and maintenance of confidentiality, privacy and security agreements as specified in this BAA 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 BAA, 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 HITECH Act in case of a need for notification by HHSC upon a determination of a Breach of Unsecured PHI as defined in the HITECH Act.
- (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 Privacy Regulations and HIPAA Security Regulations.

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

- (1) **Accounting, Access or Amendment.** 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 Person, it will promptly forward the request to HHSC; however, if it would violate HIPAA, the HIPAA Privacy Regulations or HITECH 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 the HIPAA Privacy Regulations and HIPAA Security Regulations.

- (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 security, including but not limited to, those 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 Auditing Standards No.70, Service Organizations (SAS-70) Report, or a Service Organizations Report issued in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16;
 - (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; and
 - (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.

**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 or received on behalf of HHSC, as directed by HHSC, upon termination of the BAA or Base Contract.

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

- (1) CONTRACTOR agrees that on the termination or expiration of this BAA, 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, and any data created by CONTRACTOR or any of CONTRACTOR's agents or subcontractors if that data contains Confidential Information. CONTRACTOR will certify in writing to HHSC that all the Confidential Information that has been disclosed to CONTRACTOR, and any created PHI, 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 BAA 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 use or disclose PHI in any manner that would not be permissible under HIPAA or HITECH, 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 Breached this BAA, HHSC, through its agent, will have the right to inspect the facilities, systems, books and records of CONTRACTOR to monitor compliance with this BAA. For purposes of this subsection, HHSC's agent(s) include, without limitation, the Office of the Inspector General or the Office of the Attorney General of Texas. HHSC's, through its agent's inspection, failure to inspect or failure to detect any noncompliance with the BAA does not relieve CONTRACTOR of its responsibility to comply with this BAA.

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, HIPAA Privacy Regulations, HITECH and other applicable laws and regulations of Confidential Information.

Section A5.04 *Term of BAA*

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

- (1) Either party may terminate this BAA at any time upon 30 days written notice to the other party.
- (2) HHSC may immediately terminate this BAA on:
 - (A) A material breach of this BAA. "Material" means:
 - (i) any violation by CONTRACTOR of a material term of this BAA 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 BAA;
 - (ii) CONTRACTOR fails to timely notify HHSC of an Event, Incident or Breach, or take corrective action required;
 - (iii) CONTRACTOR's repeated or flagrant violation of the obligations under the BAA;
 - (iv) CONTRACTOR's failure to respond to a demand letter concerning penalties under the BAA or Base Contract;
 - (v) CONTRACTOR being named as a defendant in a criminal proceeding for a violation of HIPAA, HIPAA Privacy Regulations, HIPAA Security Regulations, HITECH, 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, HIPAA Privacy Regulations, HIPAA Security

Regulations, HITECH, other laws and regulations of Confidential Information; or other security or privacy laws is made in any administrative or civil proceeding which CONTRACTOR has been joined.

- (vii) If neither termination or cure is feasible, HHSC shall report the violation to the Secretary.
- (3) Termination of this BAA will not relieve CONTRACTOR of its duties with regards to the return or disposition of the Confidential Information as set forth in the BAA.
- (4) **Termination Options.** If HHSC determines that CONTRACTOR has violated a material term of this BAA; HHSC may in its sole discretion:
 - (A) Exercise any of its rights including but not limited to reports, access and inspection under this BAA 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 BAA; and/or
 - (i) Provide CONTRACTOR with a reasonable period to cure the breach as determined by HHSC; or
 - (ii) Terminate the BAA 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 BAA 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 BAA and the legal relations among the Parties to this BAA 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 BAA.

Section A5.07 Injunctive Relief

- (1) CONTRACTOR understands and agrees that HHSC may suffer irreparable injury if CONTRACTOR fails to comply with any of the terms of this BAA with respect to the Confidential Information or a provision of HIPAA, HIPAA Privacy Regulations, HIPAA Security Regulations, HITECH or other laws or regulations applicable to Confidential Information.
- (2) CONTRACTOR further agrees that monetary damages may be inadequate to compensate HHSC for such 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 BAA.

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

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 BAA or from any acts or omissions related to this BAA 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 BAA 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 BAA. CONTRACTOR’s obligation to defend, indemnify and hold harmless any Indemnified Party will survive the expiration or termination of this BAA.

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 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 BAA 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 BAA, or because of an alleged dispute, breach, default, misrepresentation, or injunctive action, in connection with any of the provisions of this BAA, 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 Ag BAA 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 BAA and the Base Contract, this BAA controls.

Section A5.12 *Automatic Amendment and Interpretation*

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

ATTACHMENT 6. CONFIDENTIAL INFORMATION

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

ATTACHMENT 7. SECURITY GUIDELINES AND PROCEDURES

CONTRACTOR and all subcontractors, consultants, or agents under the BAA (collectively “CONTRACTOR”) must comply with the following Information Security Guidelines and Procedures:

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

CONTRACTOR must comply with the following, as applicable:

- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and HIPAA Privacy Regulations and HIPAA Security Regulations;
- The Health Information Technology for Economic and Clinical Health Act (HITECH Act);
- 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 Revision 3 – Recommended Security Controls for Federal Information Systems and Organizations; and
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems.

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 identified below have a demonstrated need to know and have access to Confidential Information pursuant to this BAA 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 BAA. **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: _____
Title: _____
Date: _____

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

2. Signature: _____
Name: _____
Title: _____
Date: _____

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

3. Signature: _____
Name: _____
Title: _____
Date: _____

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

4. Signature: _____
Name: _____
Title: _____
Date: _____

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

5. Signature: _____
Name: _____
Title: _____
Date: _____

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

6. Signature: _____
Name: _____
Title: _____
Date: _____

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

7. Signature: _____
Name: _____
Title: _____
Date: _____

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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