HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT OF 1996 – HIPAA AND HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT OF 2009 - HITECH

BUSINESS ASSOCIATE AGREEMENT

The Arizona Department of Economic Security (DES) or on behalf of a DES Division or Program *("DES Covered Component")*, and undersigned Business Associate hereby enter into this Business Associate Agreement *("BAA" or "Agreement").*

This BAA has the same effective date as the Contract, Intergovernmental Agreement, Memorandum of Understanding or Interagency Service Agreement to which it is appended *("Related Contract" or "Contract")*, or the date of the last signature, whichever is later. If there is no Related Contract, the effective date of this BAA is the date of the last signature to this Agreement. This Agreement supplements any Contract between a DES Covered Component and the Business Associate which involves the disclosure of Protected Health Information *("PHI")* as defined in HIPAA. In the event of conflicting terms or conditions, this Agreement's terms shall supersede the provisions of the Related Contract to which it is appended.

The DES Covered Component and the Business Associate agree to comply with applicable Privacy and Security Standards of HIPAA and HITECH, and with other applicable federal and state laws, in order to protect the privacy of PHI in any form and to safeguard the confidentiality, integrity, and availability of any Electronic PHI *("ePHI")* related to this Agreement.

1.0. DEFINITIONS. Capitalized terms not otherwise defined in this Agreement shall have the same meanings as those terms in the Privacy Rule and HITECH.

1.1 **Breach** shall have the meaning given to such term under the HITECH Act *(42 U.S.C. § 17921)*.

1.2 **Business Associate** shall have the meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act *(45 C.F.R. § 160.103 and 42 U.S.C. §17938)*.

1.3 **Covered Component** shall have the meaning given to such term under the Privacy Rule and the Security Rule *(45 C.F.R §160.103)*.

1.4 **Data Aggregation** shall have the meaning given to such term under the Privacy Rule *(45 C.F.R. §164.501)*.

1.5 **Designated Record Set** shall have the meaning given to such term under the Privacy Rule *(45 C.F.R. §164.501)*.

1.6 **Electronic Health Record** shall have the meaning given to such term in the HITECH Act *(42 C.F.R. § 17921)*.

1.7 **Electronic Protected Health Information** shall have the meaning given to such term under the Privacy Rule *(45 CFR §164.501and §106.103)*

1.8 **Health Care Operations** shall have the meaning given to such term under the Privacy Rule *(45 C.F.R. §164.501)*.

1.9 **Individual** shall have the meaning given to such term under the Privacy Rule *(45 C.F.R. §160.103)* and shall include a person who qualifies as a personal representative *(45 C.F.R. §164.502(g)*).

1.10 **Privacy Rule** shall mean the Standards for Privacy of Individually Identifiable Health Information codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

1.11 **Protected Health Information** shall have the meaning given to such term under the Privacy Rule *(45 C.F.R. §164.501)*. Protected Health Information includes Electronic Protected Health Information *(C.F.R. §160.103 and §164.501)*.

1.12 **Protected Information** shall have the meaning given to such term under the Privacy Rule *(45 C.F.R. §164.501).* Protected Information includes Electronic Protected Information *(C.F.R. §160.103 and §164.501)*.

See page 7 for EOE/ADA disclosures

1.13 **Required By Law** shall have the meaning given to such term under the Privacy Rule *(45 C.F.R. §164.512)*.

1.14 **Secretary** shall mean the Secretary of the U.S. Department of Health and Human Services or his designee.

1.15 **Security Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

1.16 **Unsecured PHI** shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act *(42 U.S.C. §17932(h)*).

2.0 PERMITTED USES AND DISCLOSURES OF PHI. The Business Associate will use and disclose PHI only for those purposes necessary to perform functions, activities, or services for, or on behalf of, the DES Covered Component as specified in the underlying Contract, this BAA , or as Required By Law. Any use or disclosure by the Business Associate shall not violate applicable Privacy Rule provisions, the terms of this BAA, or the DES Covered Component policies and procedures for using or disclosing only the Minimum Necessary PHI.

2.1 **Prohibited Use and Disclosures.** The Business Associate shall not use or disclose Protected Information for fundraising or marketing purposes. The Business Associate shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested a restriction and has paid out of pocket in full for health care items or services to which the PHI solely related as described in 42 U.S.C. §17935(a). The Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of the Covered Component and as permitted by the HITECH Act, 42 U.S.C. §17935(d) (2); however, this prohibition shall not affect payment by the Covered Component to the Business Associate for services provided pursuant to the Contract. Disclosure for research is prohibited without the Covered Component's permission prior to such disclosure.

2.2 **Business Activities of Business Associate.** The Business Associate may use PHI for the necessary management and administration of the Business Associate, or to carry out the legal responsibilities of the Business Associate if:

1. The disclosure is Required By Law; or
2. The Business Associate obtains reasonable written assurances from a third party receiving the PHI that the third party will:
   i. Maintain the confidentiality of the PHI;
   ii. Use or disclose the PHI only as Required By Law or for the purpose for which the PHI was disclosed to the person;
   iii. Notify the Business Associate within 1 business day of any discovered breach of confidentiality of the Protected Information *(42 U.S.C. §17932; 45 C.F.R. §164.504(e)(2)(ii)(D)*) and comply in writing with paragraphs 3.1, 3.2, 3.3, 3.4, 3.5 and 3.6; and
   iv. Ensure that any third party to whom it provides Protected Information receives from, or created or received by the Business Associate on behalf of the Covered Component, agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information *(45 C.F.R. §164.504 (e)(2)(ii)(D)*).

2.3. **Aggregation of PHI.** The Business Associate shall provide data aggregation services with regard to PHI created or received from or on behalf of the DES Covered Component, if requested to do so by the DES Covered Component. *(45 C.F.R. §164.504(e)(2)(i)(B)*).

2.4 **De-Identification of PHI.** Under 45 C.F.R. §164.502(d) (2), de-identified information does not constitute PHI and is not subject to the terms of this Agreement. The Business Associate may de-identify any and all PHI, provided

1. The de-identification conforms to the requirements of 45 C.F.R. §164.514(b),
2. The Business Associate maintains the documentation required by 45 C.F.R. §164.514(b), and
3. The Business Associate gives written assurance to the DES Covered Component that the Business Associate appropriately maintains the documentation required by 45 C.F.R. §164.514(b).

3.0. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.

3.1. **Safeguards.** The Business Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected information otherwise that as permitted by the Contract and the Business Associate Agreement, including, but not limited to, administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Information, in accordance with 45 C.F.R §164.308, §164.310, and §164.312. The Business Associate shall comply with the policies, procedures, and documentation requirements of the HIPAA Security Rule, including but not limited to 42 U.S.C. §17931 and 45 C.F.R. §164.316.

3.2 **Reporting Impermissible Use or Disclosure and Security Incidents.** The Business Associate agrees to report to the DES Covered Component in writing of any access, use or disclosure of Protected Information not permitted by the contract or the Business Associate Agreement, and any breach of Unsecured PHI of which it becomes aware of as described in 42 U.S.C. §17921 and 45 C.F.R. §164.308(b) and §164.504(e)(2)(ii)(C), within 1 business day after discovery. The Business Associate shall:

1. Promptly take corrective action to secure any such deficiencies; and
2. Grant prompt and immediate access to DES Covered Component and other individuals from DES or the State of Arizona authorized by DES to participate in the incident investigation, mitigation, resolution, or breach notification; and
3. Contact the DES Chief Privacy Officer if DES Covered Component cannot be notified within 1 business day after discovery of incident; and
4. Secure and preserve all records pertinent to the incident; and
5. Promptly require within 1 business day of incident discovery applicable subcontractors and agents to secure and preserve all records pertinent to the incident; and
6. Any action pertaining to such unauthorized disclosure required by applicable federal and state statutes and regulations.

3.3. **Mitigation.** The Business Associate agrees to mitigate, to the extent practicable, any harmful effects that are known to the Business Associate of a use or disclosure of PHI by the Business Associate or its agents or subcontractors in violation of the requirements of this Agreement *(45 C.F.R §164.530(f)*).

3.4 **Agents and Subcontractors.** The Business Associate agrees to the following:

1. Ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by the Business Associate on behalf of the DES Covered Component, agrees in writing to the same restrictions and conditions that apply to the Business Associate through this Agreement with respect to such PHI and implementing the safeguards required by paragraph 2.1 above with respect to Protected Information *(45 C.F.R. §164.308(b) and §164.504(e)(2)(ii)(D)*).
2. It shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violations as described in 45 C.F.R. §164.530(e)(l) and 164.530(f).

3.5 **Personnel.** The Business Associate shall appropriately inform all of its employees, agents, representatives, and members of its workforce ("Personnel"), whose services may be used to satisfy the Business Associate's obligations under this Agreement and the Related Contract, of the terms of this Agreement. The Business Associate represents and warrants that the Personnel are under sufficient legal obligations to the Business Associate for the Business Associate to fully comply with the provisions of this Agreement. The Business Associate agrees to train its workforce on the HIPAA Rule and keep appropriate records of the training as prescribed in 45 C.F.R. §164.530(b)(1)(2).

3.6. **Access to Protected Information**. The Business Associate shall make Protected Information maintained by the Business Associate or its agents or subcontractors in Designated Record Sets available to the DES Covered Component for inspection and copying within 10 business days of a request by the DES Covered Component to enable the DES Covered Component to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.524. If the Business Associate maintains an Electronic Health Record, the Business Associate shall provide such information in electronic format to enable the DES Covered Component to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. §17935(e).

3.7 **Individual Access to PHI**. If an Individual requests direct access to PHI in possession of the Business Associate which is maintained under its contract with DES, prior to disclosure of any PHI the Business Associate shall first consult in writing with the DES Covered Component's Privacy Officer or the DES Chief Privacy Officer. The Business Associate shall grant or deny access pursuant to written instructions from the DES Covered Component which are consistent with 45 C.F.R. §164.524 or other applicable law. Within 5 business days, the Business Associate shall notify the DES Covered Component's Privacy Officer or the DES Chief Privacy Officer in writing of the actions it has taken pursuant to the request for access and DES Covered Component's authorization.

3.8. **Amendment of PHI.** The Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set within 5 business days after the Business Associate receives from the DES Covered Component instructions to amend PHI. Such instructions generally follow an Individual's request to the DES Covered Component to amend the Individual's PHI held by the DES Covered Component or its Business Associates in a Designated Record Set. If the DES Covered Component declines an Individual's request to amend that Individual's PHI, the DES Covered Component shall provide to its Business Associate, who shall promptly incorporate into the Individual's Designated Record Set, any statements of disagreement and/or rebuttals supplied by the Individual, as required by 45 C.F.R. § 164.526.

3.9 **Individual Amendment of PHI**. If an individual requests an amendment of PHI directly from the Business Associate or its agents or subcontractors on behalf of the DES Covered Component, the Business Associate must notify the DES Covered Component in writing within 5 business days of the request. Any approval or denial of amendment to Protected Information maintained by the Business Associate or its agents or subcontractors shall be the responsibility of the DES Covered Component, which shall notify the Business Associate of its decision in writing.

3.10 **Documentation of Disclosure**. The Business Associate agrees to document all disclosures of PHI made by the Business Associate and information related to such disclosures as would be required by the DES Covered Component to respond to a request by an Individual for an accounting of disclosures of PHI according to 45 C.F.R. §164.528. At a minimum, the documentation related to the Business Associate's disclosure of PHI shall include:

1. The date of disclosure;
2. The name of the PHI recipient and, if known, the address of the PHI recipient;
3. A brief description of the PHI disclosed; and
4. A brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or instead of such statement, a copy of the written request for disclosure by the Secretary or under 45 C.F.R. §164.512.

3.11. **Accounting of Disclosures**. Within 10 business days after receipt of notice from the DES Covered Component to the Business Associate that the DES Covered Component has received a request for an accounting of disclosures of an Individual's PHI, the Business Associate agrees to provide the DES Covered Component with the disclosure information requested by the Individual and as required in paragraph 3.10 above. If an individual requests an accounting of disclosures directly from the Business Associate, the Business Associate shall, within sixty (60) business days, provide or deny an accounting according to 45 C.F.R §164.528. Unless otherwise directed by the DES Covered Component, the Business Associate shall notify the DES Covered Component of the action it has taken and shall do so in writing within five (5) business days after the action. The accounting of disclosure shall include all PHI disclosures for the time period the Individual requested, but not for a date earlier than six years prior to the date of creation or last entry, which ever occurred last. If the Business Associate is unable to provide the accounting of disclosure within the allowed time frame, the Business Associate shall provide the DES Covered Component with a written statement of the reason for delay and the date the Business Associate will provide the accounting.

3.12 **Government Access to Records**. For the purpose of determining the DES Covered Component compliance with the Privacy Rule, as well as the Business Associate's compliance with this BAA, the Business Associate agrees to make available to the DES Covered Component or its authorized agent, or to the Secretary, in the time and manner designated:

1. The Business Associate's internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of the DES Covered Component; and
2. All PHI received by the Business Associate from the DES Covered Component or created or received by the Business Associate on behalf of the DES Covered Component.

3.13 **Minimum Necessary**. The Business Associate and its agents and subcontractors shall request, use, and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure as described in 42 U.S.C. § 17935(b); 45 C. F. R. § 164.502(b)(1) and 164.514(d).

3.14 **Data Ownership**. The Business Associate acknowledges that the Business Associate has no ownership rights with respect to the Protected Information.

3.15 **Transaction Standards Regulation**. If the Business Associate conducts in whole or part Standard Transactions for or on behalf of the DES Covered Component, the Business Associate agrees to comply with the Electronic Data Transaction Standards and Code Sets, 45 C.F.R. Part 162 (I – R). The Business Associate agrees to require any subcontractor or agent involved in conducting Standard Transactions for or on behalf of the DES Covered Component, to comply with the Transaction Standards and Code Sets. The Business Associate and its subcontractors or agents shall not engage in any practice or enter into any agreement related to conducting in whole or in part Standard Transactions for or on behalf of the DES Covered Component that:

1. Changes the definition, Data Condition, or use of a Data Element or Segment in a Standard Transaction;
2. Adds a Data Element or Segments to the maximum defined Data Set;
3. Uses any code or Data Element that is marked “not used” in the Standard Transaction’s implementation specification or that is not in the Standard Transaction’s implementation specification; or
4. Changes the meaning or intent of the Standard transaction implementation specification.

3.16 **Retention of Records**. All records containing PHI created or received by the Business Associate from or on behalf of the DES Covered Component will be retained for six years from the date of creation *(e.g., PHI)* or the date when it last was in effect *(e.g., a policy or form)*, whichever is later.

3.17 **Violations of Law**. The Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. §164.502(j).

3.18 **Audits, Inspection and Enforcement**.

1. Within 10 business days of a written request by the DES Covered Component, the Business Associate and its agents or subcontractors shall allow the DES Covered Component to conduct a reasonable inspection of the facilities, systems, books, records, agreements, and policies and procedures relating to the use, acquisition, or disclosure of Protected Information pursuant to this Agreement for the purpose of determining whether the Business Associate has complied with this Agreement; provided, however that:
   i. The Business Associate and the DES Covered Component shall mutually agree in advance upon the scope, timing and location of such inspection. If an agreement can not be concluded, then DES will decide; and
   ii. To the extent allowed by law, the DES Covered Component shall safeguard all trade secret information of the Business Associate to which the DES Covered Component has access during the course of such inspection; and
2. The fact that the DES Covered Component inspects, fails to inspect, or has the right to inspect the Business Associate’s facilities, systems, books, records, agreements, and polices and procedures does not relieve the Business Associate of its responsibilities to comply with this Agreement. The following acts by the DES Covered Component do not constitute acceptance of such practices or waive the DES Covered Entity’s enforcement rights under the contract or Agreement.
   i. Failure to detect; or
   ii. Detection, but failure to notify the Business Associate; or
   iii. Requiring the Business Associate to correct any unsatisfactory practices.
3. The Business Associate shall notify the DES Covered Component in writing within 1 business day of learning that the Business Associate has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights.
4. Notwithstanding paragraph 3.18.1, pursuant to paragraphs 3.1 through 3.4 and in compliance with 42 U.S.C. §17921 and 45 C.F.R. §164.308(b) and §164.504(e)(2)(ii)(C), Business Associate, its subcontractors and agents shall permit prompt and immediate access to the Covered Component to all physical locations and business records, including electronic records and all relevant data files, under the control or maintained by the Business Associate, its subcontractors and agents on behalf of Covered Component, for the purpose of mitigating a data breach, conducting a risk analysis and obtaining information which will identify individuals affected.

4.0 OBLIGATIONS OF DES COVERED COMPONENT

4.1. **Notice of Privacy Practices**. The DES Covered Component shall notify the Business Associate of any changes or limitation(s) in the DES Covered Component’s Notice of Privacy Practices according to 45 C.F.R. §164.520, to the extent that such changes or limitation(s) may effect the Business Associate’s use or disclosure of PHI.

4.2 **Changes in Permission by Individual**. The DES Covered Component shall notify the Business Associate of any changes in, or revocation of, an Individual’s permission to use or disclose PHI, to the extent that such changes may affect the Business Associate’s use or disclosure of PHI.

4.3 **Restriction on PHI**. The DES Covered Component shall notify the Business Associate of any restriction on PHI uses and disclosures that the DES Covered Component has agreed to in accordance with 45 C.F.R. §164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

4.4 **Permissible Requests** by DES Covered Component. The DES Covered Component shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the DES Covered Component.

5.0 TERM AND TERMINATION

5.1 **Term**. The term of this Agreement is specified on page one (1) of this Agreement or in the Contract to which it is appended and shall terminate when all PHI provided by the DES Covered Component to the Business Associate, or created or received by the Business Associate on behalf of the DES Covered Component, is destroyed or returned to the DES Covered Component. If it is not feasible for the Business Associate to return to the DES Covered Component or destroy all PHI when this Agreement terminates under the Contract or is terminated early, protections agreed to by the Business Associate are extended to such information, whether PHI is held or controlled by the Business Associate or its agents or subcontractors.

5.2 **Effect of Termination**.

1. Except as provided in subparagraph 3 of this paragraph, upon termination of this Agreement for any reason, the Business Associate shall return or destroy all PHI received from the DES Covered Component, or created or received by the Business Associate on behalf of the DES Covered Component. No copies or data repositories can be retained as to this information.
2. This provision shall apply to PHI in the possession or under the control of subcontractors or agents of the Business Associate. The Business Associate and its subcontractors and agents shall retain no copies or data repositories of any type of returned or destroyed PHI unless ordered to do so by a court of law.
3. If the Business Associate determines that returning or destroying PHI is not feasible, the Business Associate shall provide to the DES Covered Component notification of the conditions making the return or destruction not feasible. The Business Associate shall extend the protections of this Agreement to the PHI and shall limit further uses and disclosures of the PHI to the purpose that make the return or destruction not feasible, for so long as the Business Associate maintains the PHI. If it is not feasible for the Business Associate to recover from a subcontractor or agent any PHI, the Business Associate shall provide a written explanation to the DES Covered Component. The Business Associate shall require the subcontractor or agent to agree:
   i. To extend the protections of this Agreement to the PHI in subcontractor or agent; and
   ii. To limit further uses or disclosures of the PHI to the purpose that makes the return or destruction not feasible, for so long as the subcontractor or agent maintains the PHI.

5.3 **Termination for Cause**.

1. Breach. Upon the DES Covered Component's knowledge of a material breach by the Business Associate of the terms of this Agreement, the DES Covered Component shall take one or more of the following actions:
   i. Provide an opportunity for the Business Associate to cure the breach within a specified timeframe;
   ii. Terminate this Agreement and the underlying Contract if the Business Associate does not cure the breach or end the violation within the time specified by the DES Covered Component, or if a cure of the breach is not possible;
   iii. Immediately terminate this Agreement and the underlying contract; or
   iv. Report the violation to the Secretary, if neither termination nor cure is feasible.
2. Judicial or Administrative Proceedings. The DES Covered Component may terminate the Agreement if;

i. The Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws; or
ii. There is a governmental agency or tribunal finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, the HITECH Act, the HIPAA regulations or other security or privacy laws.

6.0 MISCELLANEOUS

6.1 HIPAA Reference. A reference in this Agreement to HIPAA or the Privacy Rule means the regulation including the HITECH Act of 2009, as in effect on the effective date or as subsequently amended, and for which compliance is required. *(45 C.F.R. § 160, §162, and §164 and 42 U.S.C. §17938)*.

6.2. **Amendment**. The parties agree to take the action necessary to amend this Agreement from time to time so that the DES Covered Component may comply with the requirements of HIPAA, HITECH, court decisions and any regulatory changes.

6.3 **Interpretation**. Any ambiguity in this Agreement shall be resolved to permit the DES Covered Component to comply with the HIPAA and HITECH Rules.

Contractor hereby acknowledges receipt and acceptance of this HIPAA Business Associate Agreement and that a signed copy must be filed with the DES Procurement Office.	**The above referenced HIPAA Business Associate Agreement is hereby executed this**
Signature _____ Date _____	**day of** _____ **20**____ **by the**
Printed Name _____	**Department of Economic Security.**
Title _____	DES Senior Records and Privacy Officer Signature
Name of Contractor _____	_____