HIPAA BUSINESS ASSOCIATE AGREEMENT

This **Business Associate Agreement** ("BAA"), effective _____ ("Effective Date"), is entered into by and between _____, a [STATE] [ENTITY TYPE] ("Business Associate") and _____, a [STATE] [ENTITY TYPE] ("Covered Entity") (Business Associate and Covered Entity each referred to herein as a "Party" and collectively as the "Parties").

WHEREAS, Business Associate has an arrangement to provide services on behalf of one or more organizations identified as a Covered Entity under 45 CFR § 160.103; and

WHEREAS, pursuant to an agreement dated _____ (the "Primary Agreement") Business Associate provides _____ services ("Services") to or for Covered Entity; and

WHEREAS, in the course of providing the Services, Covered Entity may make available to Business Associate, or have Business Associate obtain on its behalf, information that may be deemed Protected Health Information (PHI) subject to the provisions of HIPAA.

NOW THEREFORE, in consideration of the mutual promises set forth in this BAA, and other good and valuable consideration, the sufficiency and receipt of which is hereby acknowledged, the Parties agree as follows:

1. **Definitions.**
   - **(a)** Capitalized terms used but not otherwise defined in this BAA shall have the meanings ascribed in HIPAA (whether or not such terms are capitalized therein) or elsewhere in the Primary Agreement, as the case may be.
   - **(b)** "Breach" means any use or disclosure of PHI not provided for by the Primary Agreement, including breaches of unsecured protected health information as required by 45 C.F.R. § 164.610.
   - **(c)** "PHI" means Protected Health Information received by Business Associate from or on behalf of Covered Entity or created by Business Associate for or on behalf of Covered Entity.

2. **Permitted Uses.** Business Associate may use PHI only as permitted or required by this BAA for the following purposes: (i) as necessary to provide the Services; (ii) to carry out its legal responsibilities; (iii) for the proper business management and administration of Business Associate; (iv) to provide data aggregation services relating to the health care operations of Covered Entity to the extent necessary or requested to provide the Services; and (v) as required by law.

3. **Permitted Disclosures.** Business Associate may disclose PHI only as permitted or required by this BAA for the following purposes: (i) as necessary to provide the Services; (ii) for the proper business management and administration of Business Associate or to carry out its legal responsibilities, if Business Associate has obtained reasonable assurances that the recipient will (A) hold such PHI in confidence, (B) use or further disclose it only for the purpose for which it was received or as Required By Law, and (C) notify Business Associate

of any instance of which the recipient becomes aware in which the confidentiality of such PHI has been breached; (iii) for the proper business management and administration of Business Associate or to carry out its legal responsibilities, if required by law; and (iv) as otherwise required by law; provided, however, that any disclosure to an agent or subcontractor of Business Associate shall be pursuant to a written agreement between Business Associate and such agent or subcontractor containing substantially the same restrictions and conditions on the use and disclosure of PHI as are set forth in this BAA.

4. **Prohibited Uses and Disclosures.** Business Associate shall not use or further disclose PHI in a manner that would violate HIPAA if done by the Covered Entity. Business Associate shall not sell PHI or use or disclose PHI for purposes of marketing or fundraising. Unless Covered Entity gives its prior, express written consent, Business Associate shall not de-identify any PHI except as necessary to provide the Services and unless expressly provided otherwise in a written agreement between the Parties, (i) as between Business Associate and Covered Entity, all de-identified PHI shall be and remain exclusively the property of Covered Entity, (ii) Business Associate assigns to Covered Entity all of Business Associate's right, title, and interest therein, if any, and (iii) Business Associate shall not use any such de-identified PHI for any purpose other than to provide the Services and shall not disclose the same to any third party except with the prior written consent of Covered Entity or as otherwise required by applicable law or upon the order of a court of competent jurisdiction.

5. **Safeguards.** Business Associate shall establish and maintain appropriate safeguards intended to prevent use or disclosure of PHI other than as provided in this BAA. Without limiting the foregoing, Business Associate shall establish and maintain, in compliance with HIPAA and any applicable guidance issued pursuant thereto, administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any PHI that is Electronic Protected Health Information or any other Electronic Protected Health Information maintained or transmitted by Business Associate for or on behalf of Covered Entity, and Business Associate shall establish and maintain policies and procedures and comply with the documentation requirements set forth in HIPAA.

6. **Reports to Covered Entity; Breach Notification.**

   (a) Without unreasonable delay and in no case later than ten (10) days after discovering a Breach involving PHI that is Unsecured Protected Health Information, Business Associate shall report such Breach to Covered Entity in writing, setting forth the date of discovery thereof, the identities of affected individuals (or, if such identities are unknown at that time, the classes of such individuals), a general description of the nature of the incident, and such other information as is required pursuant to HIPAA or reasonably requested by Covered Entity. For purposes hereof, a Breach shall be deemed discovered by Business Associate when it is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate.

   (b) Business Associate shall report to Covered Entity in writing any use or disclosure of PHI that is not permitted by this BAA, other than a Breach involving PHI that is Unsecured Protected Health Information, within thirty (30) days of Business Associate's discovery thereof.

(c) Business Associate shall report to Covered Entity in writing any Security Incident involving PHI that is Electronic Protected Health Information within thirty (30) days of Business Associate's discovery thereof. The Parties acknowledge and agree that this section requires notice by Business Associate to Covered Entity of the ongoing occurrence of incidents that may constitute Security Incidents but that are trivial and do not result in unauthorized access, use, or disclosure of PHI that is Electronic Protected Health Information, including pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, and denials of service, for which no additional notice to Covered Entity shall be required.

7. **Reimbursement; Mitigation.** Business Associate shall reimburse Covered Entity for all reasonable and necessary out-of-pocket costs incurred by Covered Entity to provide required notices of a Breach involving PHI that is Unsecured Protected Health Information, and Business Associate shall take all actions reasonably necessary and cooperate with Covered Entity as reasonably requested to mitigate, to the extent practicable, any harmful effects of such occurrence.

8. **Minimum Necessary.** Business Associate shall request, use, and disclose only the minimum amount of PHI necessary to provide the Services.

9. **Access and Amendment.** With respect to an Individual as to whom Business Associate maintains PHI, Business Associate shall notify Covered Entity promptly upon receipt of a request from such an Individual for access to or a copy of such Individual's PHI or to amend such Individual's PHI. To the extent permitted under HIPAA, and except as otherwise required upon the order of a court of competent jurisdiction, (i) Business Associate shall direct such Individual to make such request of Covered Entity and (ii) Business Associate shall not consent to such access, deliver such copy, or comply with such request except as directed by Covered Entity. With respect to PHI maintained by Business Associate in a Designated Record Set, to the extent required by HIPAA of a Covered Entity, Business Associate shall (i) make available PHI to Individuals or Covered Entity or to a third party designated by such Individual, in writing, as requested by Covered Entity and in accordance with HIPAA, and (ii) upon receipt of notice from Covered Entity, promptly amend any portion of the PHI so that Covered Entity may meet its amendment obligations under HIPAA.

10. **Accounting for Disclosures.** Business Associate shall document all disclosures of PHI by Business Associate and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with HIPAA. Business Associate shall maintain such information for the applicable period set forth in HIPAA. Business Associate shall deliver such information to Covered Entity or, upon Covered Entity's request, to the Individual, in the time and manner reasonably designated by Covered Entity, in order for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with HIPAA. The obligations set forth in this section shall survive the expiration or any termination of this BAA and shall continue, as to a given instance of a disclosure, until the earlier of (i) the

passing of the time required for such information to be maintained pursuant to HIPAA or (ii) the delivery to Covered Entity of all such information in a form and medium reasonably satisfactory to Covered Entity and the return or destruction of all PHI as provided in this BAA.

11. **Additional Restrictions.** If Covered Entity notifies Business Associate that Covered Entity has agreed to be bound by additional restrictions on the uses or disclosures of PHI pursuant to HIPAA, Business Associate shall be bound by such additional restrictions and shall not use or disclose PHI in violation of such additional restrictions.

12. **Audit.** If Business Associate receives a request, made on behalf of the Secretary of the Department of Health and Human Services, that Business Associate make its internal practices, books, and records relating to the use or disclosure of PHI available to the Secretary of the Department of Health and Human Services for the purposes of determining Covered Entity's or Business Associate's compliance with HIPAA, Business Associate promptly shall notify Covered Entity of such request and, unless enjoined from doing so by order of a court of competent jurisdiction in response to a challenge raised by Covered Entity or Business Associate (which challenge Business Associate shall not be obligated to raise), Business Associate shall comply with such request to the extent required of it by applicable law. Nothing in this BAA shall waive any attorney-client privilege or other privilege applicable to either Party.

13. **Remuneration.** Business Associate shall not receive remuneration, directly or indirectly, in exchange for PHI; provided, however, that this prohibition shall not affect payment to Business Associate by Covered Entity pursuant to the Primary Agreement.

14. **Obligations of Covered Entity.** Covered Entity shall (i) notify Business Associate of any limitation in Covered Entity's Notice of Privacy Practices to the extent that such limitation may affect Business Associate's use or disclosure of PHI, (ii) notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such change may affect Business Associate's use or disclosure of PHI, (iii) notify Business Associate of any restriction on the use or disclosure of PHI to which Covered Entity has agreed in accordance with HIPAA, to the extent that such restriction may affect Business Associate's use or disclosure of PHI, and (iv) obtain any authorization or consents as may be Required by Law for any of the uses or disclosures of PHI necessary for Business Associate to provide to the Services.

15. **Termination.** This BAA shall continue in effect until the earlier to occur of (i) expiration or termination of the Primary Agreement or (ii) termination pursuant to this section. Either Party may terminate this BAA effective immediately if it determines that the other Party has breached a material provision of this BAA and failed to cure such breach within thirty (30) days of being notified by the other Party of the breach. If the non-breaching Party reasonably determines that cure is not possible, such Party may terminate this BAA effective immediately upon written notice to other Party.

16. Effect of Termination. Upon termination of this BAA, Business Associate shall deliver to Covered Entity the disclosure accounting information as provided in this BAA and (i) if feasible, return to Covered Entity or destroy, as provided in the Agreement, all PHI that Business Associate maintains in any form and retain no copies of such PHI, or (ii) if return or destruction is not feasible (including if Business Associate is required by applicable law to retain any such PHI for a time following termination), notify Covered Entity and extend the protections of this BAA to the PHI and limit its further use or disclosure to those purposes that make the return or destruction of the PHI infeasible. The requirements of this section shall survive termination or expiration of this BAA and shall be in force as long as any PHI remains in the custody or control of Business Associate.

17. Miscellaneous.

(a) Amendments. Upon the enactment of any law or regulation affecting the use or disclosure of PHI, or on the publication of any decision of a court of competent jurisdiction relating to any such law, or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, Covered Entity may, by written notice to Business Associate, propose to amend this BAA in such a manner as Covered Entity reasonably determines necessary to comply therewith, and such proposed amendment shall become operative unless Business Associate rejects such amendment by written notice to Covered Entity within thirty (30) days thereafter, in which case, unless the Parties agree on an amendment within thirty (30) days after Business Associate's notice, either Party may terminate this BAA by written notice to the other.

(b) Interpretation. In the event of a conflict between the provisions of this BAA and any other provisions of the Primary Agreement, the provisions of this BAA shall control. In the event of an inconsistency between the provisions of this BAA and any mandatory provisions of HIPAA, as amended, or its interpretation by any court or regulatory agency with authority over either party hereto, HIPAA (interpreted by such court or agency, if applicable) shall control. Where provisions of this BAA are different than those mandated under HIPAA, but are nonetheless permitted by such rules as interpreted by relevant courts or agencies, the provisions of this BAA shall control.

IN WITNESS WHEREOF, Business Associate and Covered Entity have each caused this **Business Associate Agreement** to be duly executed in its name and on its behalf effective as of the Effective Date.

BUSINESS ASSOCIATE

By: _____

Its: _____

COVERED ENTITY

By: _____

Its: _____