BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT ("BAA" or "Agreement") is made and entered into this _____day of _____, _____, by and between _____ ("Covered Entity"), whose business address is _____, and _____ ("Business Associate"), whose business address is _____.

RECITALS

A. Covered Entity is a Covered Entity as that term is defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, and the related regulations promulgated by the Department of Health and Human Services Act ("HHS"), (collectively "HIPAA"), and as such is required to comply HIPAA's provisions regarding the confidentiality and Privacy of Protected Health Information ("PHI").

B. Covered Entity and Business Associate have entered into one or more agreements under which Business Associate provides or will provide certain specified services to Covered Entity (i.e., collectively the Agreement).

C. In providing services pursuant to the Agreement, Business Associate Business Associate will have access to PHI.

D. By providing the services pursuant to the Agreement, the Business Associate will become a Business Associate of the Covered Entity, as that term is defined under the Health Insurance Portability and Accountability Act ("HIPAA").

E. Both parties intend to protect the privacy and security of PHI disclosed to the Business Associate pursuant to the terms of this Agreement, HIPAA, and other applicable laws.

F. Covered Entity is required by the Privacy Rule and the Security Rule issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to obtain satisfactory assurance that Business Associate will appropriately safeguard the protected health information ("PHI") received from, or created or received on behalf of, Covered Entity.

AGREEMENT

NOW, THEREFORE, In consideration of the mutual covenants and conditions contained herein and the continued provision of PHI by the Covered Entity to the Business Associate under the Agreement in reliance on this BAA, the parties agree as follows:

SECTION 1. Definitions

1.1 **"Affiliate" means a subsidiary or affiliate of a** Covered Entity that is, or has been, considered a covered entity, as defined by HIPAA.

1.2 **"Breach"** means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, which compromises the privacy or security of the PHI, as defined in 45 CFR 164.402.

1.3 "**Breach Notification Rule."** See the definition outlined in Subpart D of 456 CFR Part 164.

1.4 **"Business Associate**" shall generally have the same meaning as "business associate" at 45 CFR 160.103. In this Agreement, Business Associate shall also mean [INSERT BUSINESS ASSOCIATE NAME].

1.5 **"Covered Entity**" shall generally have the same meaning as "covered entity" at 45 CFR 160.103. In this Agreement, Covered Entity shall also mean [INSERT COVERED ENTITY NAME].

1.6 "**Data Aggregation**" means, concerning PHI created or received by the Business Associate in its capacity as the "business associate" under HIPAA of Covered Entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in itscapacity as a business associate of one or more other "covered entity" under HIPAA, to permitdata analyses that relate to the Health Care Operations (defined below) of the respective covered entities. The meaning of "data aggregation" in this BAA shall be consistent with the meaning given to that term in the Privacy Rule.

1.7 "**Designated Record Set**" has the meaning given to such term under the Privacy Rule,including 45 CFR §164.501.

1.8 "**De-Identify**" means to alter the PHI such that the resulting information meets therequirements described in 45 CFR §§164.514(a) and (b).

1.9 "**Electronic PHI"** means any PHI maintained in or transmitted by electronic media asdefined in 45 CFR §160.103

1.10 "**Health Care Operations**" has the meaning given to that term in 45 CFR §164.501.

1.11 "**HHS**" means the U.S. Department of Health and Human Services.

1.12 "**HITECH ACT**" means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.

1.13 **"Individual**" shall have the same meaning as the term "Individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative by 45 CFR 164.502(g).

1.14 "**Privacy Rule**" shall mean the standards for privacy of Individually Identifiable Health Information at 45 CFR Part 160 and 164, Subparts A and E.

1.15 "**Security Rule**" shall mean the standards for security of electronic PHI at 45 CFR Parts 160 and 164, Subparts A and C.

1.16 "**Security Incident**" means the attempt or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

1.17 **"Protected Health Information**" ("PHI") shall have the same meaning as the term "Protected Health Information" in 45 CFR 164.501, limited to the information received from, or created or received by Business Associate on behalf of, Covered Entity.

1.18 **"Secretary"** shall mean the Department of Health and Human Services Secretary or his/her designee.

1.19 **"Unsecured Protected Health Information**" or "**Unsecured PHI"** means any "protected health information" as defined in 45 CFR §§164.501 and 160.103 that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS Secretary in the guidance issued under the HITECH Actand codified at 42 USC §17932(h).

SECTION 2. Uses and Disclosures of PHI

2.1 Except as otherwise provided in this BAA, the Business Associate may use or disclose PHI as reasonably necessary to provide the services described in the Agreement to the Covered Entity and to undertake other activities permitted or required of the Business Associate by this BAA or as required by law.

2.2 Except as otherwise limited by this BAA or federal or state law, the Covered Entity authorizes the Business Associate to use the PHI to properly manage and administer the Business Associate's business and carry out its legal responsibilities. Business Associate may disclose PHI for its proper management and administration, provided that (i) the disclosures are required by law; or (ii) Business Associate obtains, in writing, before making any disclosure to a third party (a) reasonable assurances from this third party that the PHI will be held confidential as provided under this BAA and used or further disclosed only as required by law or for the purpose for which it was disclosed to this third party and (b) an agreement from this third party to notify Business Associate immediately of any breaches of the confidentiality of the PHI, to the extent it knows of the breach.

2.3 Business Associate will not use or disclose PHI in a manner other than as provided in thisBAA, as permitted under the Privacy Rule, or as required by law. Business Associate will use or disclose PHI, to the extent practicable, as a limited data set or limited to the minimum necessary amount of PHI to carry out the intended purpose of the use or disclosure, by Section 13405(b) of the HITECH Act (codified at 42 USC §17935(b)) and any of the act's implementing regulations adopted by HHS, for each use or disclosure of PHI.

2.4 Upon request, the Business Associate will make any of the Covered Entity's PHI available to the Covered Entity that the Business Associate or any of its agents or subcontractors possess.

2.5 Business Associates may use PHI to report violations of law to appropriate Federal andState authorities, consistent with 45 CFR §164.502(j)(1).

2.6 **Agreements with Agents or Subcontractors**. Business Associate will ensure that any of its agents or subcontractors that have access to, or to which Business Associate provides PHI agree in writing to the restrictions and conditions concerning uses and disclosures of PHI contained in this BAAand agree to implement reasonable and appropriate safeguards to protect any Electronic PHI that it creates, receives, maintains or transmits on behalf of Business Associate or, through the Business Associate, Covered Entity. Business Associate shall notify Covered Entity, or upstream Business Associate, of all subcontracts and agreements relating to the Agreement, where the subcontractor or agent receives PHI as described in section 1.17 of this BAA. Such notification shall occur within 30 (thirty) calendar days of the execution of the subcontract by placement of such notice on the BusinessAssociate's primary website. By 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, the Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate concerning such information.

2.7 **Use Safeguards.** Business Associate agrees to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 to prevent the use or disclosure of PHI other than as provided by this Agreement. Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic PHI ("ePHI") that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate agrees to take reasonable steps, including providing adequate training to its employees to ensure compliance with thisBAA and that the actions or omissions of its employees or agents do not cause Business Associate to breach the terms of this BAA.

2.8 **Report Unpermitted Disclosures of PHI and Security Incidents.** Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for or permitted by this Agreement of which it becomes aware, including any Breach of unsecured PHI as required at 45 CFR 164.410, and any security incident of which it becomes aware. The business associate shall report any potential breach to the covered entity without unreasonable delay and within five business days of discovering a breach. Business Associate shall further handle breach notifications to Individuals, the HHS Office of Civil Rights ("OCR"), and potentially the media on behalf of the Covered Entity. BusinessAssociate will reimburse Covered Entity for any costs incurred by it in complying with the requirements of Subpart D of 45 CFR §164 imposed on Covered Entity as a result of a Breach committed by Business Associate.

2.9 **Reporting Breaches of Unsecured PHI**. Business Associate will notify Covered Entity in writing promptly upon the discovery of any Breach of Unsecured PHI in accordance with the requirements set forth in 45 CFR 164.410, but in no case later than 30 days after discovery of the Breach. Business Associate will reimburse Covered Entity for any costs incurred by it in complying with the requirements of Subpart D of 45 CFR 164 imposed on Covered Entity as a result of a Breach committed by Business Associate.

2.10 **Mitigation of Disclosure of PHI**. Business Associate will take reasonable measures to mitigate, to the extent practicable, any harmful effect known to Business Associate of any use or

disclosure of PHI by Business Associate or its agents or subcontractors in violation of the requirements of this BAA.

2.11 Audit Report. Upon request, the Business Associate will provide the Covered Entity, or upstream Business Associate, with a copy of its most recent independent HIPAA compliance report (AT-C 315), HITRUST certification, or other mutually agreed upon independent standards-based third-party audit report. Covered Entity agrees not to re-disclose Business Associate's audit report.

2.12 Disclose Practices, Books, and Records. Unless otherwise protected or prohibited from discovery or disclosure by law, the Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining the Covered Entity's compliance with the Privacy Rule or the Security Rule. Business Associate shall have a reasonable time to comply with requests for such access. In no case shall access be required in less than five business days after the Business Associate's receipt of such request unless otherwise designated by the Secretary.

2.13 Respond to Requests from Individuals. Except as this Agreement or any other agreement between Covered Entity and Business Associate may otherwise provide, if Business Associate receives an access, amendment, accounting of disclosure, or other similar request directly from an Individual, Business Associate will redirect Individual to Covered Entity.

2.14 Access to PHI by Individuals.

A. Upon request, the Business Associate agrees to furnish the Covered Entity with copies of the PHI maintained by the Business Associate in a Designated Record Set in the time and manner designated by the Covered Entity to enable the Covered Entity to respond to an Individual's request for access to PHI under 45 CFR §164.524.

B. In the event any Individual or personal representative requests access to the Individual's PHI directly from the Business Associate, the Business Associate will forward that request to the Covered Entity within ten business days. Any disclosure of, or decision not to disclose, the PHI requested by an Individual or a personal representative and compliance with the requirements applicable to an Individual's right to obtain access to PHI shall be the sole responsibility of the Covered Entity.

2.15 Amendment of PHI.

A. Upon request and instruction from Covered Entity, Business Associate will amend PHI ora record about an Individual in a Designated Record Set that is maintained by, or otherwise within the possession of, Business Associate as directed by Covered Entity in accordance with procedures established by 45 CFR §164.526. Business Associate will complete any request by Covered Entity to amend such information within 15 business days of Covered Entity'srequest.

B. If any Individual requests that the Business Associate amend such Individual's PHI or record in a Designated Record Set, the Business Associate, within ten business days, will forward this request to the Covered Entity. Any amendment of, or decision not to amend, the PHI or record as requested by an Individual and compliance with the requirements applicable to an Individual's right to request an amendment of PHI will

be the sole responsibilityof the Covered Entity.

2.16 Accounting Disclosures

A. Business Associate will document any disclosures of PHI made by it to account for such disclosures as required by 45 CFR §164.528(a). Business Associate also will make available information related to such disclosures as would be necessary for the Covered Entity to respond to arequest for an accounting of disclosures in accordance with 45 CFR §164.528. At a minimum, Business Associate will furnish Covered Entity the following with respect to any covered disclosures by Business Associate: (i) the date of disclosure of PHI; (ii) the name of the entity orperson who received PHI, and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure which includes the basis for such disclosure.

B. Business Associate will furnish to Covered Entity information collected in accordance with this Section, within ten business days after written request by Covered Entity, to permit Covered Entity to make an accounting of disclosures as required by 45 CFR §164.528, or if Covered Entity elects to provide an Individual with a list of its business associates, Business Associate will provide an accounting of its disclosures of PHI upon request of the Individual, if and to the extent that such accounting is required under the HITECH Act or HHS regulations adopted in connection with the HITECH Act.

C. If an Individual delivers the initial request for an accounting directly to a Business Associate, the Business Associate will forward the request to the Covered Entity within ten business days.

2.17 Availability of Books and Records. Upon request, the Business Associate will make available its internal practices, books, agreements, records, and policies and procedures relating to the use and disclosure of PHI to the Secretary of HHS to determine the Covered Entity's and Business Associate's compliance with HIPAA and this BAA.

2.18 Responsibilities of Covered Entity. With regard to the use and/or disclosure of Protected HealthInformation by the Business Associate, the Covered Entity agrees to:

A. Notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such restriction may affect BusinessAssociate's use or disclosure of PHI.

B. Notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes mayaffect Business Associate's use or disclosure of PHI.

C. Notify the Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

D. Except for data aggregation or management and administrative activities of the Business Associate, the Covered Entity shall not request the Business Associate to use or disclose

PHI in any manner that would not be permissible under HIPAA if done by the Covered Entity.

2.19 Data Ownership. Business Associate's data stewardship does not confer data ownership rights on Business Associate with respect to any data shared with it under the Agreement, including any forms thereof.

SECTION 3. Permitted Uses and Disclosures by Business Associate.

3.1 Business Associate may use or disclose PHI for the following purposes: As necessary to perform the services agreed to between the Parties, notwithstanding the restrictions on such uses and disclosures set forth in HIPAA and this Agreement.

3.2 Business Associate may only de-identify PHI if permitted by Covered Entity and, in any event, may only de-identify PHI in accordance with 45 CFR 164.514(a)-(c).

3.3 Business Associate may use or disclose PHI as required by law or where Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3.4 Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity except for the specific uses and disclosures set forth herein.

SECTION 4. Provision for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions.

4.1 Limitations in Notice of Privacy Practices. The Covered Entity shall notify the Business Associate of any limitation(s) in the notice of privacy practices of the Covered Entity under 45 CFR 164.520 to the extent that such limitation may affect the Business Associate's use or disclosure of PHI.

4.2 Changes in or Revocation of Permission to Use PHI. The Covered Entity shall notify the Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

4.3 Restriction on Use or Disclosure of PHI. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

SECTION 5. Term and Termination

5.1 Term. The Term of this Agreement shall be effective as of the date both parties signed this Agreement and shall terminate when (a) all obligations of the parties have been met under this

Agreement or BAA, or (b) all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is not feasible to return or destroy PHI in the determination of Business Associate, protections are extended to such information, by the termination provisions in this Section.

5.2 Termination for Cause.

A. Upon Covered Entity's reasonable determination that Business Associate has breached or violated a material term of this Agreement, Covered Entity shall give Business Associate written notice of such breach and provide reasonable opportunity, not to exceed 15 days, for Business Associate to cure the breach or end the violation. The covered Entity may terminate the Agreement, and the Business Associate agrees to such termination if the Business Associate has breached a material term of this Agreement and does not cure the breach in the period provided or if cure is not possible. Covered Entity may report the problem to the Secretary of HHS if termination is not feasible.

B. If the Business Associate determines that the Covered Entity has breached a material term of this BAA, then the Business Associate will provide the Covered Entity with written notice of the existence of the breach and shall provide the Covered Entity with 30 days to cure the breach. Covered Entity's failure to remedy the breach within the 30-day period will be grounds for immediate termination of the Agreement and this BAA by Business Associate. Business Associate may report the breach to HHS.

5.3 Effect of Termination. Upon termination of the Agreement or this BAA for any reason, all PHI maintained by the Business Associate will be returned to the Covered Entity or destroyed by the Business Associate. Business Associate will not retain any copies of such information. This provision will apply to PHI in the possession of Business Associate's agents and subcontractors. If return or destruction of the PHI is not feasible, in the Business Associate's reasonable judgment, the Business Associate will furnish the Covered Entity with notification, in writing, of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of the PHI is infeasible, Business Associate will extend the protections of this BAA to such information for as long as Business Associate retains such information and will limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible.

5.4 Survival. The rights and obligations of the Business Associate under section 5 of this Agreement shall survive the termination of this Agreement.

SECTION 6. Miscellaneous

6.1 Entire Agreement. This Agreement supersedes all prior and contemporaneous written and oral agreements and understandings regarding this subject matter between the Covered Entity and Business Associate. It contains the entire agreement between the parties.

6.2 Amendment. The parties agree to take such action as necessary to amend this Agreement from time to time for compliance with the HIPAA Rules. This Agreement may only be amended by the parties' signed written agreement.

6.3 Severability. If any provision or provisions of this Agreement is/are determined by a court of competent jurisdiction to be unlawful, void, or unenforceable, this Agreement shall not be illegal, void, or unenforceable. Still, it shall continue in effect and be enforced as such provision or provisions were omitted.

6.4 Waiver. A waiver concerning one event shall not be construed as continuing or as a bar to or waiver of any right or remedy as to subsequent events.

6.5 Other Agreements. All other agreements entered into by the parties hereto, not related to this subject matter, remain in full force and effect.

6.6 Governing Law. This Agreement and the rights of the parties hereunder shall be governed by and construed in accordance with the laws of the State of _____, exclusive of conflict or choice of law rules.

6.7 Regulatory References. A reference in this BAA to a section in HIPAA means the section is in effect or as amended at the time.

6.8 Effect of BAA. This BAA is part of and subject to the terms of the Agreement, except that to the extent any terms of this BAA conflict with any term of the Agreement, the terms of this BAA will govern. Except as expressly stated in this BAA or as provided by law, this BAA will not create any rights in favor of any third party.

6.9 HITECH Act Compliance. The Parties acknowledge that the HITECH Act includes significant changes to the Privacy and Security Rule. The privacy subtitle of the HITECH Act sets forth provisions that significantly change the requirements for business associates and the agreements between business associates and covered entities under HIPAA. These changes may be further clarified in forthcoming regulations and guidance. Each Party agrees to comply with the applicable provisions of the HITECH Act and any HHS regulations issued concerning the HITECH Act. The Parties also agree to negotiate in good faith to modify this BAA as reasonably necessary to comply with the HITECH Act and its regulations as they become effective. Still, if the Parties cannot agree on such a modification, either Party will have the right to terminate this BAA upon 30 days' prior written notice to the other Party.

6.10 Notices. All notices, requests, and demands or other communications to be given under this BAAto a Party will be made via either first class mail, registered or certified or express courier, or electronic mail to the Party's address given below:

A. If to Covered Entity:

Attn: _____
Address: _____
Email: _____

B. If to Business Associate:

Attn: _____
Address: _____
Email: _____

APPROVED AND ACCEPTED:

COVERED ENTITY

By: _____ **Date:** _____
NAME:
TITLE:

BUSINESS ASSOCIATE

By: _____ **Date**: _____
NAME:
TITLE: