HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is made as of this __ day of _____ (the "Effective Date") by and between _____ ("Covered Entity" or CE") and _____ ("Business Associate" or "BA") (each a "party" and, collectively, the "parties").

1. **PREAMBLE AND DEFINITIONS.**

1.1 Pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended (**"HIPAA"**), You (**"Covered Entity"**) and Us, or any of our corporate affiliates where applicable (**"Business Associate"**) enter into this Business Associate Agreement (**"BAA"**) that addresses the HIPAA requirements with respect to "business associates," as defined under the privacy, security, breach notification, and enforcement rules at 45 C.F.R. Part 160 and Part 164 (**"HIPAA Rules"**). A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.

1.2 This BAA is intended to ensure that Business Associate will establish and implement appropriate safeguards for the Protected Health Information (**"PHI"**) (as defined under the HIPAA Rules) that Business Associate may receive, create, maintain, use, or disclose in connection with the functions, activities, and services that Business Associate performs for Covered Entity. The functions, activities, and services that Business Associate performs for Covered Entity are defined in the Master Service Agreement, together with Schedules, Exhibit, and Addenda now existing or hereinafter entered into (the **"Underlying Agreement"**).

1.3 Pursuant to changes required under the Health Information Technology for Economic and Clinical Health Act of 2009 (the **"HITECH Act"**) and under the American Recovery and Reinvestment Act of 2009 (**"ARRA"**), this BAA also reflects federal breach notification requirements imposed on Business Associate when "Unsecured PHI" (as defined under the HIPAA Rules) is acquired by an unauthorized party, and the expanded privacy and security provisions imposed on business associates.

1.4 Unless the context clearly indicates otherwise, the following terms in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, disclosure, Electronic Media, Electronic Protected Health Information (ePHI), Health Care Operations, individual, Minimum Necessary, Notice of Privacy Practices, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured PHI, and use.

1.5 A reference in this BAA to the Privacy Rule means the Privacy Rule, in conformity with the regulations at 45 C.F.R. Parts 160-164 (the **"Privacy Rule"**) as interpreted under applicable regulations and guidance of general application published by the HHS, including all amendments thereto for which compliance is required, as amended by the HITECH Act, ARRA, and the HIPAA Rules.

2. **GENERAL OBLIGATIONS OF BUSINESS ASSOCIATE**.

2.1 Business Associate agrees not to use or disclose PHI, other than as permitted or required by this BAA, the Underlying Agreement or as Required By Law, or if such use or disclosure does not otherwise cause a Breach of Unsecured PHI.

2.2 Business Associate agrees to use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI, to prevent use or disclosure of PHI other than as provided for by the BAA.

2.3 Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate as a result of a use or disclosure of PHI by Business Associate in violation of this BAA's requirements or that would otherwise cause a Breach of Unsecured PHI.

2.4 The Business Associate agrees to the following breach notification requirements:

(a) During the term of the Underlying Agreement: To notify You (i) as soon as is reasonably possible by telephone call plus email or fax upon the discovery ("discovery" within the meaning of the HITECH Act) of breach of security of PHI in computerized form if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person, or (ii) within 24 hours by email or fax of the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of the Underlying Agreement and this Schedule, or potential loss of confidential data affecting this Agreement. Business Associate shall take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

(b) To investigate any security incident, breach, or unauthorized use or disclosure of PHI or confidential data

within 72 hours of such a breach, and when the investigation is complete to disclose to You (i) what data elements were involved and the extent of the data involved in the breach, and (ii) provide and discovered information regarding the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data, (iii) a description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized, (iv) a description of the probable causes of the improper use or disclosure; and (v) whether the potential exists that federal or state laws requiring individual notifications of breaches may have been triggered.

(c) Business Associate shall provide information reasonably requested by Covered Entity for purposes of investigating the Breach and any other available information that Covered Entity is required to include to the individual under 45 C.F.R. § 164.404(c) at the time of notification or promptly thereafter as information becomes available.

(d) Business Associate's notification of a Breach of Unsecured PHI under this Section shall comply in all respects with each applicable provision of Section 13400 of Subtitle D (Privacy) of ARRA, the HIPAA Rules and related guidance issued by the Secretary or the delegate of the Secretary from time to time.

2.5 Business Associate agrees, in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, to require 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 with respect to such information.

2.6 Business Associate agrees to make available PHI in a Designated Record Set to the "covered entity" as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524.

(a) Business Associate agrees to comply with an individual's request to restrict the disclosure of their personal PHI in a manner consistent with 45 C.F.R. § 164.522, except where such use, disclosure, or request is required or permitted under applicable law.

(b) Business Associate agrees that when requesting, using, or disclosing PHI in accordance with 45 C.F.R. § 164.502(b)(1) that such request, use, or disclosure shall be to the minimum extent necessary, including the use of a "limited data set" as defined in 45 C.F.R. § 164.514(e)(2), to accomplish the intended purpose of such request, use, or disclosure, as interpreted under related guidance issued by the Secretary from time to time.

2.7 Business Associate agrees to make any amendments to PHI in a Designated Record Set as agreed to by the Covered Entity pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526.

2.8 Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.528.

2.9 Business Associate agrees to make its internal practices, books, and records, including policies and procedures regarding PHI, relating to the use and disclosure of PHI and Breach of any Unsecured PHI received from Covered Entity, or created or received by the Business Associate on behalf of Covered Entity, available to Covered Entity (or the Secretary) for the purpose of Covered Entity or the Secretary determining compliance with the Privacy Rule (as defined in Section 8).

2.10 To the extent that Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate agrees to comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

2.11 Business Associate agrees to account for the following disclosures:

(a) Business Associate agrees to maintain and document disclosures of PHI and Breaches of Unsecured PHI and any information relating to the disclosure of PHI and Breach of Unsecured PHI in a manner as would be required for Covered Entity to respond to a request by an individual or the Secretary for an accounting of PHI disclosures and Breaches of Unsecured PHI.

(b) Business Associate agrees to provide to Covered Entity information collected in accordance with this Section 2.11, to permit Covered Entity to respond to a request by an individual or the Secretary for an accounting of PHI disclosures and Breaches of Unsecured PHI.

(c) Business Associate agrees to account for any disclosure of PHI used or maintained as an Electronic Health

Record (as defined in Section 5) (**"EHR"**) in a manner consistent with 45 C.F.R. § 164.528 and related guidance issued by the Secretary from time to time; provided that an individual shall have the right to receive an accounting of disclosures of EHR by the Business Associate made on behalf of the Covered Entity only during the three years prior to the date on which the accounting is requested from Covered Entity.

2.12 Business Associate agrees to comply with the "Prohibition on Sale of Electronic Health Records or Protected Health Information," as provided in Section 13405(d) of Subtitle D (Privacy) of ARRA, and the "Conditions on Certain Contacts as Part of Health Care Operations," as provided in Section 13406 of Subtitle D (Privacy) of ARRA and related guidance issued by the Secretary from time to time.

3. **PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE**.

3.1 General Uses and Disclosures. Business Associate agrees to receive, create, use, or disclose PHI only in a manner that is consistent with this BAA, the Underlying Agreement, the Privacy Rule, or Security Rule (as defined in Section 5); provided that the use or disclosure would not violate the Privacy Rule, including 45 C.F.R. § 164.504(e), if the use or disclosure would be done by Covered Entity.

3.2 Business Associate may use or disclose PHI as Required By Law.

3.3 Business Associate may (i) use and disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached, and (ii) use PHI to provide data aggregation services to Our customers. Data aggregation means the combining and de-identifying of PHI created or received by the Business Associate from You, or PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit health data and analyses features and products to be created and sold to Our customers. Business Associate may also Use PHI to report violations of law to appropriate Federal and State authorities, consistent with applicable law.

3.4 Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity.

4. **OBLIGATIONS OF COVERED ENTITY**.

4.1 Covered Entity shall:

(a) Provide Business Associate with the Notice of Privacy Practices that Covered Entity produces in accordance with the Privacy Rule, and any changes or limitations to such notice under 45 C.F.R. § 164.520, to the extent that such changes or limitations may affect Business Associate's use or disclosure of PHI.

(b) Notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI under this BAA.

(c) Notify Business Associate of any changes in or revocation of permission by an individual to use or disclose PHI, if such change or revocation may affect Business Associate's permitted or required uses and disclosures of PHI under this BAA.

4.2 Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy and Security Rule if done by Covered Entity, except as provided under Section 3 of this BAA.

5. **COMPLIANCE WITH SECURITY RULE**.

5.1 Business Associate shall comply with the HIPAA Security Rule, which shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. Part 160 and Subparts A and C of Part 164, as amended by ARRA and the HITECH Act. The term **"Electronic Health Record"** or **"EHR"** as used in this BAA shall mean an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

5.2 In accordance with the Security Rule, Business Associate agrees to:

(a) Implement the administrative safeguards set forth at 45 C.F.R. § 164.308, the physical safeguards set forth at 45 C.F.R. § 164.310, the technical safeguards set forth at 45 C.F.R. § 164.312, and the policies and procedures set forth at 45 C.F.R. § 164.316 to reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Security Rule.

(b) Require that any agent, including a Subcontractor, to whom it provides such PHI agrees to implement reasonable and appropriate safeguards to protect the PHI; and

(c) Report to the Covered Entity any Security Incident of which it becomes aware.

6. **INDEMNIFICATION**.

The parties agree and acknowledge that except as set forth herein, the indemnification obligations contained under the Underlying Agreement shall govern each party's performance under this BAA.

7. **TERM AND TERMINATION**.

7.1 Upon termination of the Underlying Agreement, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, the terms of the Underlying Agreement relating to return, destruction, and/or transition of PHI will govern. Covered Entity agrees that the Underlying Agreement is sufficient, compliant, reasonable, and meets requirements of the law. Covered Entity releases Business Associate from any liability arising from matters relating to the return, destruction, and/or transition of PHI upon termination of the Underlying Agreement.

8. **MISCELLANEOUS**.

8.1 The parties agree to take such action as is necessary to amend this BAA to comply with the requirements of the Privacy Rule, the Security Rule, HIPAA, ARRA, the HITECH Act, the HIPAA Rules, and any other applicable law.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement:

BUSINESS ASSOCIATE	**COVER ENTITY**
_____	_____
BY:	**BY:**
Title:	**Title:**
Date:	**Date:**