Business Associate Agreement

(Covered Entity Version)

This Business Associate Agreement ("Agreement") dated ____, [year] is between _____ ("Covered Entity") and _____ ("Business Associate").

Catch-all Definition

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Regulations: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. Capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in HIPAA, HIPAA Regulations and HITECH.

Specific Definitions

Business Associate shall be defined as provided in 45 CFR Sections160.103. Generally, a business associate means a person who, on behalf of a covered entity, creates, receives, maintains, or transmits PHI or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity. A covered entity may be a business associate of another covered entity. A business associate includes, among other things, a person that offers a personal health record to one or more individuals on behalf of a covered entity and/or a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate. In reference to this Agreement, Business Associate shall mean [insert Name of Business Associate].

Covered Entity shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean [Insert Name of Covered Entity].

HIPAA shall be defined herein as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191

HIPAA Regulations shall be defined herein as the regulations promulgated under HIPAA by the United States Department of Health and Human Services ("HHS"), including but not limited to, 45 CFR Part 160 and 45 CFR Part 164, as are currently in effect or as later amended. In the event that a regulatory citation to HIPAA contained within this Agreement should change prior to this Agreement being amended, the regulatory citation in this Agreement shall be deemed to have been changed to the new citation.

HITECH shall be defined herein as the Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111–5. In the event that a regulatory citation to HITECH contained within this Agreement should change prior to this Agreement being amended, the regulatory citation in this Agreement shall be deemed to have been changed to the new citation.

Privacy Rule shall be defined herein as the standards of privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

Security Rule shall be defined herein as the standards of security requirements of the HIPAA Regulations at Subpart C of 45 CFR Part 164.

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

Obligations and Activities of Business Associate

Privacy Use or Disclosure. Business Associate agrees not to use or disclose Protected Health Information, ("PHI") in violation of this Agreement or as required by law. Business Associate agrees to comply with the requirements of 45 CFR Section 164.502 and shall use and disclose PHI obtained pursuant to this Agreement in compliance with each requirement of 45 CFR §164.502.

Prohibited Payment for PHI. Business Associate agrees to not directly or indirectly receive payment in exchange for any PHI, unless Covered Entity obtained from the individual, who is the subject of the PHI, a signed written authorization specifically stating that the PHI can be exchanged for payment, or otherwise permitted by the limited exceptions as provided in HITECH §13405(d).

Mitigation. Business Associate agrees to mitigate, to the extent reasonably possible, any harmful effect that is known to Business Associate from any use or disclosure of PHI by Business Associate, or a subcontractor or agent of Business Associate, that is not authorized by this Agreement. Business Associate further agrees to mitigate, to the extent reasonably possible, any harmful effect that is known to Business Associate from any Security Incident or, after a reasonable investigation, would be known to Business Associate.

Training of Workforce. Business Associate shall train the members of its workforce whose function involves contact with PHI to appropriately handle and safeguard PHI. Such training shall, at a minimum, include: implementation and use of risk assessment criteria to determine when a Breach occurs, and how to report a Breach.

Subcontractors and Agents. Business Associate may disclose protected health information to a business associate that is a subcontractor or agent and may allow the subcontractor or agent to create, receive, maintain, or transmit PHI on its behalf, if the Business Associate obtains satisfactory assurances, in accordance with 45 CFR §164.502(e)(1)(ii) & §164.308(b)(2), that the subcontractor or agent will appropriately safeguard the information by imposing, at a minimum, the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

Audit/Inspection. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate, or subcontractor or agent of Business Associate, on behalf of Covered Entity available to the Covered Entity or the Secretary or his/her designee in a timely manner for purposes of determining compliance with the HIPAA Regulations.

Access. Business Associate agrees to provide timely access, when requested by Covered Entity, to PHI in a Designated Record Set (if PHI is maintained in a Designated Record Set) to Covered Entity or an individual for purposes of compliance with 45 CFR §164.524 and Covered Entity's policies.

Notice of Inspection Business Associate shall notify Covered Entity of any requests or demands for inspection made by the HHS for information related to Covered Entity with respect to Covered Entity's compliance with the HIPAA. Business Associate also agrees to make available to the HHS its internal policies and procedures, books, and records with respect to the HHS's demand.

Amendment. Provided Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR 164.526 and Covered Entity's policies in the time and manner directed by Covered Entity at the request of Covered Entity or an Individual.

Documentation of Disclosures. Business Associate agrees to document such disclosures of PHI 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 45 CFR § 164.528 and Covered Entity's policies. Business Associate agrees to provide to

Covered Entity or an Individual, in a timely manner, information collected in accordance with this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

Security Rule. Business Associate agrees to comply with the requirements of the Security Rule in the same manner that such sections apply to Covered Entity. Business Associate agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect PHI, as required by the Security Rule. Any Business Associate agent or subcontractor will also implement such safeguards. Business Associate agrees to conduct a risk assessment and implement reasonable administrative, technical, and physical safeguards designed to protect both Covered Entity's PHI and other business and other proprietary information from unauthorized disclosure. Business Associate agrees to update the risk assessment and related safeguards at least annually. Upon request by Covered Entity, Business Associate agrees to provide documentation sufficient to demonstrate its compliance with the terms of this Agreement.

Privacy Rule. Business Associate agrees to comply with the requirements of the Privacy Rule Subpart E of 45 CFR Part 164) to the extent Business Associate carries out one or more of Covered Entity's obligation(s) under the Privacy Rule

Reporting Security Incidents & Breaches. Business Associate agrees to report to Covered Entity (1) any use or disclosure of PHI not provided for by this Agreement, (2) any suspected use or disclosure of PHI not provided for by this Agreement and (3) any Security Incident of which it becomes aware, including any Breach of unsecured PHI as required by 45 CFR §164.410. Business Associate shall make this report to the Covered Entity within 2 business days after it becomes aware of, or has a reasonable suspicion of, a use or disclosure covered by this paragraph (the "Report"). The Report shall be made to the persons identified in Exhibit A to this Agreement. Business Associate shall be deemed to have knowledge of a Security Incident and/or a Breach if the relevant facts are known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Security Incident/Breach, who is an employee, officer, or other agent of the Business Associate.

Content Of Report. When Business Associate reports any use or disclosure of PHI not provided for by this Agreement to Covered Entity, the Report shall include: (1) a description of the Breach or Security Incident; (2) a description of the content of the PHI involved (e.g., date of birth, Social Security number); (3) if known, the identity of the person or persons who were responsible for the Breach or Security Incident; (4) a description of the steps Business Associate has taken to identify the cause of the Breach; (5) an outline of any corrective action(s) implemented to prevent a future Breach or Security Incident; (6) a recommendation on how Business Associate and/or Covered Entity can help mitigate harm from the Breach or Security Incident; and, (7) contact information for those individuals at Business Associate available to discuss the Breach or Security Incident.

Information Provided to Covered Entity. Business Associate shall provide to the Covered Entity, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during the Security Incident and/or Breach. In addition, Business Associate shall provide the Covered Entity with any other available information that the Covered Entity is required to include in notification to the individual under 45 CFR §164.404(c) or as soon thereafter as information becomes available. Business Associate shall cooperate with Covered Entity and assist Covered Entity in its obligations to notify Individuals, the media or any other required entity. Covered Entity shall determine the extent to which such notification(s) may be required. Covered Entity shall bear full responsibility for making such notifications to Individuals and/or the media (unless delegated to Business Associate in writing). Business Associate shall cover or reimburse Covered Entity for any and all costs associated with the foregoing notification(s). Covered Entity retains the final right of approval of any and all communications to its patients, employees, media, regulators or any other party for whom Covered Entity may be obligated to notify.

Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI as required by law and to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in Exhibit "B" attached hereto, which may be amended in writing and signed by the parties, provided that such use or disclosure would not violate HIPAA, HIPAA Regulations, HITECH or the policies and procedures of Covered Entity if done by Covered Entity. Business Associate agrees to make uses and disclosures and requests for PHI consistent with Covered Entity's minimum necessary policies and procedures. Business Associate may not use or disclose PHI in a manner that would violate the Privacy Rule (Subpart E of 45 CFR Part 164) if done by covered entity.

Obligations of Covered Entity

Covered Entity shall provide Business Associate with its notice of privacy practices prepared to comply with 45 CFR 164.520, and any changes to such notice.

Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect Business Assocate's use or disclosure of PHI.

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would violate the Privacy Rule, HIPAA Regulations, or this Agreement.

Covered Entity will be responsible for notifications arising out of Security Incidents and/or Breach including notifications to individuals, the HHS Office of Civil Rights, the media, and any other interested party.

Term and Termination

Term. This Agreement shall be effective as of ***[Insert Effective Date]***, and shall terminate when 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 infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

Termination by Covered Entity for Cause. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall either: (1) provide an opportunity for Business Associate to cure the breach or end the violation; or (2) immediately terminate the Agreement. In any event, this Agreement will terminate if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity. If neither termination nor cure is feasible, Covered Entity shall report the violation to the HHS.

Termination by Business Associate for Cause. Upon Business Associate's knowledge of a violation by Covered Entity of the Privacy Rule, Business Associate shall terminate this Agreement for cause.

Effect of Termination.

1. Upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall also apply to PHI that is in the possession of, or created or received by, subcontractors or agents of Business Associate. Business Associate, including any subcontractor or agent of Business Associate, shall retain no copies of the PHI.

2. In the event that Business Associate or its subcontractor or agent determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon agreement by the parties that return or destruction of PHI is not feasible; Business

Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

Miscellaneous

Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the rules and requirements of applicable law protecting the privacy, security and confidentiality of PHI including but not limited to HIPAA, HIPAA Regulations and any regulations later promulgated pursuant to HIPAA. All amendments must be made in writing and signed by all parties to this Agreement.

Survival. The respective rights and obligations of Business Associate of this Agreement shall survive the termination of this Agreement.

No Third Party Beneficiaries. This Agreement shall not create any rights for any third parties not expressly identified herein, including, but not limited to any third party beneficiary who may be receiving benefits pursuant to the terms and conditions of any group health plan or contract of insurance.

Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity and Business Associate to comply with the rules and requirements of applicable law protecting the privacy, security and confidentiality of PHI including but not limited to HIPAA, HIPAA Regulations and HITECH.

State Law. Nothing in this Agreement shall require Business Associate to use or disclose PHI without proper authorization under applicable state law for such use or disclosure.

Indemnity. Business Associate agrees to indemnify, hold harmless and defend Covered Entity from and against any and all claims, losses, liabilities, costs and other expenses incurred as a result of, or arising directly or indirectly out of or in connection with: (1) violation of any term or duty imposed by this Agreement; (2) any claims, demands, awards, judgments, actions and proceedings made by any person, organization or government agency arising out of or in any way connected with violation of any term or duty imposed by this Agreement; and (3) any Security Incident or Breach of PHI while such PHI was in the possession of Business Associate or its agents and subcontractors. Covered Entity shall have the option, at its sole discretion, to employ attorneys selected by it to defend any such action, or to provide advice regarding breach notification, the costs and expenses of which shall be the responsibility of Business Associate. Covered Entity shall provide Business Associate with timely notice of the existence of such proceedings and such information, documents and other cooperation as reasonably necessary to assist Business Associate in establishing a defense to such action. These indemnities shall survive termination of this Agreement.

Insurance. Business Associate agrees to purchase and maintain at all times during the term of this agreement a professional liability insurance policy and a privacy and data security insurance policy covering it and each subcontractor or agent. Each policy of insurance must identify Covered Entity as an additional named insured. The professional liability policy shall provide insurance limits of at least $_____ per occurrence and $_____ aggregate. The privacy and data security insurance policy shall provide insurance limits of at least $_____ per occurrence and $_____ aggregate.

Authority. The undersigned representative acknowledges and warrants that he/she has the authority to bind the entity Business Associate.

Covered Entity	**Business Associate**
Company Name: _____	Company Name: _____
By: _____	By: _____
Printed Name: _____	Printed Name: _____
Its (title): _____	Its (title): _____
Date: _____ / _____ / _____	Date: _____ / _____ / _____

Exhibit "A"

[Insert the names and contact information of the individuals at your company who should be notified in the event of a breach or security incident.]

Exhibit “B”

[Insert permitted use and disclosure by Business Associate.]