



HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“**BAA**”) is entered into effective this ___ day of _____ 20__ (“**Effective Date**”) by and between and _____ (“**Business Associate**”)(each a “**Party**” and collectively, the “**Parties**”).

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 104-91), as amended, (“**HIPAA**”), and the regulations promulgated thereunder by the Secretary of the U.S. Department of Health and Human Services (“**Secretary**”), including, without limitation, the regulations codified at 45 C.F.R. Parts 160 and 164 (“**HIPAA Regulations**”);

B. Business Associate performs Services for or on behalf of Covered Entity, and in performing said Services; Business Associate creates, receives, maintains, or transmits Protected Health Information (“**PHI**”);

C. The Parties intend to protect the privacy and provide for the security of PHI Disclosed by Covered Entity to Business Associate, or received or created by Business Associate, when providing Services in compliance with HIPAA, the Health Information Technology for Economic and Clinical Health Act (Public Law 111-005) (“the **HITECH Act**”) and its implementing regulations and guidance issued by the Secretary, and other applicable state and federal laws, all as amended from time to time; and

D. As a Covered Entity, Covered Entity is required under HIPAA to enter into a BAA with Business Associate that meets certain requirements with respect to the Use and Disclosure of PHI, which are met by this BAA.

AGREEMENT

In consideration of the Recitals and for other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the Parties agree as follows:

I.

DEFINITIONS

The following terms shall have the meaning set forth below. Capitalized terms used in this BAA and not otherwise defined shall have the meanings ascribed to them in HIPAA, the HIPAA Regulations, or the HITECH Act, as applicable.

- I.1. “**Breach**” shall have the meaning given under 42 U.S.C. § 17921(1) and 45 C.F.R. § 164.402.
- I.2. “**Designated Record Set**” shall have the meaning given such term under 45 C.F.R. § 164.501.
- I.3. “**Disclose**” and “**Disclosure**” mean, with respect to PHI, the release, transfer, provision of access to, or divulging in any other manner of PHI outside of Business Associate or to other than members of its Workforce, as set forth in 45 C.F.R. § 160.103.
- I.4. “**Electronic PHI**” or “**e-PHI**” means PHI that is transmitted or maintained in electronic media, as set forth in 45 C.F.R. § 160.103.
- I.5. “**Protected Health Information**” and “**PHI**” mean any information, whether oral or recorded in any form or medium, that: (a) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; (b) identifies the individual (or for which there is a reasonable basis for believing that the information can be used to identify the individual); and (c) shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. § 160.103. Protected Health Information includes e-PHI.
- I.6. “**Security Incident**” shall have the meaning given to such term under 45 C.F.R. § 164.304.
- I.7. “**Services**” shall mean the services for or functions on behalf of Covered Entity performed by Business Associate pursuant to any service agreement(s) between Covered Entity and Business Associates which may be in effect now or from time to time (“**Underlying Agreement**”), or, if no such agreement is in effect, the services or functions performed by Business Associate that constitute a Business Associate relationship, as set forth in 45 C.F.R. § 160.103.
- I.8. “**Unsecured PHI**” shall have the meaning given to such term under 42 U.S.C. § 17932(h), 45 C.F.R. § 164.402, and guidance issued pursuant to the HITECH Act including, but not limited to the guidance issued on April 17, 2009 and published in 74 Federal Register 19006 (April 27, 2009) by the Secretary.

I.9. “Use” or “Uses” mean, with respect to PHI, the sharing, employment, application, utilization, examination or analysis of such PHI within Business Associate’s internal operations, as set forth in 45 C.F.R. § 160.103.

I.10. “Workforce” shall have the meaning given to such term under 45 C.F.R. § 160.103.

II.

OBLIGATIONS OF BUSINESS ASSOCIATE

II.1. Permitted Uses and Disclosures of Protected Health Information Business Associate shall not Use or Disclose PHI other than for the for the purposes listed on the signature page hereto for performing the Services, as permitted or required by this BAA, or as Required by Law. Business Associate shall not Use or Disclose PHI in any manner that would constitute a violation of Subpart E of 45 C.F.R. Part 164 if so Used or Disclosed by Covered Entity. However, Business Associate may Use or Disclose PHI (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate, provided that with respect to any such Disclosure either: (a) the Disclosure is Required by Law; or (b) Business Associate obtains a written agreement from the person to whom the PHI is to be Disclosed that such person will hold the PHI in confidence and will not Use and further Disclose such PHI except as Required by Law and for the purpose(s) for which it was Disclosed by Business Associate to such person, and that such person will notify Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached; (iii) for Data Aggregation purposes for the Health Care Operations of Covered Entity. To the extent that Business Associate carries out one or more of Covered Entity’s obligations under Subpart E of 45 C.F.R. Part 164, Business Associate must comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligations.

II.2. Prohibited Marketing and Sale of PHI Notwithstanding any other provision in this BAA, Business Associate shall comply with the following requirements: (i) Business Associate shall not Use or Disclose PHI for fundraising or marketing purposes, except to the extent expressly authorized or permitted by this BAA and consistent with the requirements of 42 U.S.C. § 17936, 45 C.F.R. §§ 164.514(f), and 164.508(a)(3)(ii), and (iii) Business Associate shall not directly or indirectly receive remuneration in exchange for PHI except with the prior written consent of Covered Entity and as permitted by the HITECH Act, 42 U.S.C. § 17935(d)(2), and 45 C.F.R. § 164.502(a)(5)(ii).

II.3. Adequate Safeguards of PHI Business Associate shall implement and maintain appropriate safeguards to prevent Use or Disclosure of PHI other than as provided for by this BAA. Business Associate shall reasonably and appropriately protect the confidentiality, integrity, and availability of e-PHI that it creates, receives, maintains or

transmits on behalf of Covered Entity in compliance with Subpart C of 45 C.F.R. Part 164 to prevent Use or Disclosure of PHI other than as provided for by this BAA.

II.4. Mitigation Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this BAA.

II.5. Reporting Non-Permitted Use or Disclosure

II.5.1. Reporting Security Incidents and Non-Permitted Use or Disclosure

Business Associate shall report to Covered Entity in writing each Security Incident or Use or Disclosure that is made by Business Associate, members of its Workforce or Subcontractors that is not specifically permitted by this BAA no later than three (3) business days after becoming aware of such Security Incident or non-permitted Use or Disclosure, in accordance with the notice provisions set forth herein. Business Associate shall investigate each Security Incident or non-permitted Use or Disclosure of Covered Entity's PHI that it discovers to determine whether such Security Incident or non-permitted Use or Disclosure constitutes a reportable Breach of Unsecured PHI. Business Associate shall document and retain records of its investigation of any Breach, including its reports to Covered Entity under this Section 2.5.1. Upon request of Covered Entity, Business Associate shall furnish to Covered Entity the documentation of its investigation and an assessment of whether such Security Incident or non-permitted Use or Disclosure constitutes a reportable Breach. If such Security Incident or non-permitted Use or Disclosure constitutes a reportable Breach of Unsecured PHI, then Business Associate shall comply with the additional requirements of Section 2.5.2 below.

II.5.2. Breach of Unsecured PHI If Business Associate determines that a reportable Breach of Unsecured PHI has occurred, Business Associate shall provide a written report to Covered Entity without unreasonable delay but no later than thirty (30) calendar days after discovery of the Breach. To the extent that information is available to Business Associate, Business Associate's written report to Covered Entity shall be in accordance with 45 C.F.R. §164.410(c). Business Associate shall cooperate with Covered Entity in meeting Covered Entity's obligations under the HITECH Act with respect to such Breach. Covered Entity shall have sole control over the timing and method of providing notification of such Breach to the affected individual(s), the Secretary and, if applicable, the media, as required by the HITECH Act. Business Associate shall reimburse Covered Entity for its reasonable costs and expenses in providing the notification, including, but not limited to, any administrative costs associated with providing notice, printing and mailing costs, and costs of mitigating the harm (which may include the costs of obtaining credit monitoring services and identity theft insurance) for affected individuals whose PHI has or may have been compromised as a result of the Breach.

II.6. Availability of Internal Practices, Books, and Records to Government Business Associate agrees to make its internal practices, books and records relating to the Use and Disclosure of PHI received from, or created or received by the Business Associate on behalf of Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with HIPAA, the HIPAA Regulations, and the HITECH Act. Except to the extent prohibited by law, Business Associate shall notify Covered Entity of all requests served upon Business Associate for information or documentation by or on behalf of the Secretary. Business Associate agrees to provide to Covered Entity proof of its compliance with the HIPAA Security Standards.

II.7. Access to and Amendment of Protected Health Information To the extent that Business Associate maintains a Designated Record Set on behalf of Covered Entity and within fifteen (15) days of a request by Covered Entity, Business Associate shall (a) make the PHI it maintains (or which is maintained by its Subcontractors) in Designated Record Sets available to Covered Entity for inspection and copying, or to an individual to enable Covered Entity to fulfill its obligations under 45 C.F.R. § 164.524, or (b) amend the PHI it maintains (or which is maintained by its Subcontractors) in Designated Record Sets to enable the Covered Entity to fulfill its obligations under 45 C.F.R. § 164.526. Business Associate shall not Disclose PHI to a health plan for payment or Health Care Operations purposes if and to the extent that Covered Entity has informed Business Associate that the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates, consistent with 42 U.S.C. § 17935(a) and 42 C.F.R. § 164.522(a)(1)(vi). If Business Associate maintains PHI in a Designated Record Set electronically, Business Associate shall provide such information in the electronic form and format requested by the Covered Entity if it is readily reproducible in such form and format, and, if not, in such other form and format agreed to by Covered Entity to enable Covered Entity to fulfill its obligations under 42 U.S.C. § 17935(e) and 45 C.F.R. § 164.524(c)(2). Business Associate shall notify Covered Entity within fifteen (15) days of receipt of a request for access to PHI.

II.8. Accounting To the extent that Business Associate maintains a Designated Record Set on behalf of Covered Entity, within thirty (30) days of receipt of a request from Covered Entity or an individual for an accounting of disclosures of PHI, Business Associate and its Subcontractors shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under 45 C.F.R. § 164.528 and its obligations under 42 U.S.C. § 17935(c). Business Associate shall notify Covered Entity within fifteen (15) days of receipt of a request by an individual or other requesting party for an accounting of disclosures of PHI.

II.9. Use of Subcontractors Business Associate shall require each of its Subcontractors that creates, maintains, receives, or transmits PHI on behalf of Business Associate, to execute a Business Associate Agreement that imposes on such Subcontractors the same

restrictions, conditions, and requirements that apply to Business Associate under this BAA with respect to PHI.

II.10. Minimum Necessary Business Associate (and its Subcontractors) shall, to the extent practicable, limit its request, Use, or Disclosure of PHI to the minimum amount of PHI necessary to accomplish the purpose of the request, Use or Disclosure, in accordance with 42 U.S.C. § 17935(b) and 45 C.F.R. § 164.502(b)(1) or any other guidance issued thereunder.

III.

TERM AND TERMINATION

III.1. Term The term of this Agreement shall be effective as of the Effective Date and shall terminate as of the date that 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 the PHI, protections are extended to such information, in accordance with Section 3.3, or on the date that Covered Entity terminates for cause as authorized in Section 3.2, whichever is sooner.

III.2. Termination for Cause Upon Covered Entity's knowledge of a material breach or violation of this BAA by Business Associate, Covered Entity shall either:

a. Notify Business Associate of the breach in writing, and provide an opportunity for Business Associate to cure the breach or end the violation within ten (10) business days of such notification; provided that if Business Associate fails to cure the breach or end the violation within such time period to the satisfaction of Covered Entity, Covered Entity may immediately terminate this BAA upon written notice to Business Associate; or

b. Upon written notice to Business Associate, immediately terminate this BAA if Covered Entity determines that such breach cannot be cured.

III.3. Disposition of Protected Health Information Upon Termination or Expiration

III.3.1. Upon termination or expiration of this BAA, Business Associate shall either return or destroy all PHI received from, or created or received by Business Associate on behalf of Covered Entity, that Business Associate still maintains in any form and retain no copies of such PHI. If Covered Entity requests that Business Associate return PHI, PHI shall be returned in a mutually agreed upon format and timeframe, at no additional charge to Covered Entity

III.3.2. If return or destruction is not feasible, Business Associate shall (a) retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities; (b) return to

Covered Entity the remaining PHI that Business Associate still maintains in any form; (c) continue to extend the protections of this BAA to the PHI for as long as Business Associate retains the PHI; (d) limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction of the PHI infeasible and subject to the same conditions set out in Section 2.1 and 2.2 above, which applied prior to termination; and (e) return to Covered Entity the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

IV.

MISCELLANEOUS

IV.1. Amendment to Comply with Law This BAA shall be deemed amended to incorporate any mandatory obligations of Covered Entity or Business Associate under the HITECH Act and its implementing HIPAA Regulations. Additionally, the Parties agree to take such action as is necessary to amend this BAA from time to time as necessary for Covered Entity to implement its obligations pursuant to HIPAA, the HIPAA Regulations, or the HITECH Act.

IV.2. Indemnification Business Associate hereby agrees to indemnify and hold harmless Covered Entity, its affiliates, and their respective officers, directors, managers, members, shareholders, employees and agents from and against any and all fines, penalties, damage, claims or causes of action and expenses (including, without limitation, court costs and attorney's fees) arising from any violation of HIPAA, the HIPAA Regulations, or the HITECH Act or from any negligence or wrongful acts or omissions, including but not limited to failure to perform its obligations, that results in a violation of HIPAA, the HIPAA Regulations, or the HITECH Act, by Business Associate or its employees, directors, officers, subcontractors, agents or members of Business Associate's Workforce.

IV.3. Notices Any notices required or permitted to be given hereunder by either Party to the other shall be given in writing: (1) by personal delivery; (2) by electronic mail or facsimile with confirmation sent by United States first class registered or certified mail, postage prepaid, return receipt requested; (3) by bonded courier or by a nationally recognized overnight delivery service; or (4) by United States first class registered or certified mail, postage prepaid, return receipt, in each case, addressed to a Party on the signature page(s) to this Agreement or to such other addresses as the Parties may request in writing by notice given pursuant to this Section 4.3. Notices shall be deemed received on the earliest of personal delivery; upon delivery by electronic facsimile with confirmation from the transmitting machine that the transmission was completed; twenty-four (24) hours following deposit with a bonded courier or overnight delivery service; or seventy-two (72) hours following deposit in the U.S. mail as required herein.

IV.4. Relationship of Parties Business Associate is an independent contractor and not an agent of Covered Entity under this BAA. Business Associate has the sole right and obligation to supervise, manage, contract, direct, procure, perform or cause to be performed all Business Associate obligations under this BAA.

IV.5. Survival The respective rights and obligations of the Parties under Sections 3.3 and 4.2 of this BAA shall survive the termination of this BAA.

Applicable Law and Venue This Agreement shall be governed by and construed in accordance with the laws of the ADD YOUR STATE (without regards to conflict of laws principles). The Parties agree that all actions or proceedings arising in connection with this BAA shall be tried and litigated exclusively in the State or federal (if permitted by law and if a Party elects to file an action in federal court) courts located in ADD YOUR COUNTY.

The Parties hereto have duly executed this as of the Effective Date.

For BUSINESS ASSOCIATE Name:

By: _____

Print Name: _____

Title: _____

Dated: _____

For COVERED ENTITY:

Organization Name: _____

By: _____

Print Name: _____

Title: _____

Dated: _____

Notice Address:

attn: _____

fax: _____

email: _____

Notice Address:

attn: _____

fax: _____

email: _____