

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the “Agreement”) is effective as of (the “Agreement Effective Date”) by and between (“CE”) and (“BA”).

RECITALS

WHEREAS, CE has engaged BA to perform services or provide goods, or both;

WHEREAS, CE possesses Individually Identifiable Health Information that is protected under HIPAA (as hereinafter defined) and the HIPAA Regulations (as hereinafter defined), and is permitted to use or disclose such information only in accordance with HIPAA and the HIPAA Regulations;

WHEREAS, BA may receive such information from CE, or create and receive such information on behalf of CE, in order to perform certain of the services or provide certain of the goods, or both; and

WHEREAS, CE wishes to ensure that BA will appropriately safeguard Individually Identifiable Health Information;

NOW THEREFORE, CE and BA agree as follows:

1. **Definitions.** The parties agree that the following terms, when used in this Agreement, shall have the following meanings, provided that the terms set forth below shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in HIPAA and the HIPAA Regulations.

a. “*Business Associate*” means, with respect to a Covered Entity, a person who:

(1) on behalf of such Covered Entity or of an organized health care arrangement (as defined under the HIPAA Regulations) in which Covered Entity participates, but other than in the capacity of a member of the workforce of such Covered Entity or arrangement, performs, or assists in the performance of:

a) a function or activity involving the use or disclosure of Individually Identifiable Health Information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

b) any other function or activity regulated by the HIPAA Regulations; or

(2) provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which Covered Entity participates, where the provision of the service involves the disclosure of Individually Identifiable Health Information from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

b. “*Covered Entity*” means a health plan (as defined by HIPAA and the HIPAA Regulations), a health care clearinghouse (as defined by HIPAA and the HIPAA Regulations), or a health care provider (as defined by HIPAA and the HIPAA Regulations) who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Regulations.

c. “*Data Aggregation*” means the combining, by the Business Associate, of the Covered Entity’s PHI with PHI that the Business Associate received from another Covered Entity, to permit data analyses that relate to the health care operations of the respective Covered Entities.

d. “*HIPAA*” means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

e. “*HIPAA Regulations*” means the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164.

f. “*Individually Identifiable Health Information*” means information that is a subset of health information, including demographic information collected from an individual, and;

(1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) 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; and

a) that identifies the individual; or

b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

g. “*PHI*” means Protected Health Information that: (i) Business Associate receives from CE; (ii) Business Associate creates for its own purposes from Protected Health Information that Business Associate receives from CE; or (iii) is created, received, transmitted or maintained by Business Associate on behalf of CE.

h. “*Protected Health Information*” means Individually Identifiable Health Information that is transmitted by electronic media; maintained in any medium described in the definition of the term *electronic media* in the HIPAA Regulations; or transmitted or maintained in any other form or medium. Protected Health Information excludes Individually Identifiable Health Information in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g, and records described at 20 U.S.C. § 1232g(a)(4)(B)(iv).

i. “*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.

2. **Status of Parties.** BA hereby acknowledges and agrees that CE is a Covered Entity and that BA is a Business Associate of CE.

3. **Permitted Uses and Disclosures.**

a. *Performance of Services.* BA may use and disclose PHI in connection with the performance of the services [listed in Exhibit A attached to this Agreement] [provided in Agreement] if such use or disclosure of PHI would not violate HIPAA or the HIPAA Regulations if done by Covered Entity or such use or disclosure is expressly permitted under Section 3.b. or 3.c. of this Agreement.

b. *Proper Management and Administration.* BA may use PHI for the proper management and administration of BA in connection with the performance of services described in Exhibit A attached to this Agreement and as permitted by this Agreement. BA may disclose CE’s PHI for such proper management and administration of BA only with the prior consent of CE. Any such disclosure of PHI shall only be made if BA obtains reasonable assurances from the person to whom the PHI is disclosed that: (1) the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and (2) BA will be notified by such person of any instances of which it becomes aware in which the confidentiality of the PHI has been breached.

c. [INCLUDE ONLY IF BA WILL BE DOING DATA AGGREGATION FOR CE; OTHERWISE DELETE] [Except as otherwise limited in this Agreement, BA may use PHI to provide Data Aggregation services to CE as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B). Data Aggregation services involve the combining by BA of (a) PHI with (b) Protected Health Information received by BA in its capacity as a business associate of another Covered Entity, to permit data analyses that relate to the health care operations of the respective Covered Entities.]

4. **Nondisclosure.**

a. *As Provided In Agreement.* BA shall not use or further disclose CE's PHI except as permitted or required by this Agreement.

b. *Disclosures Required By Law.* BA shall not, without the prior written consent of CE, disclose any PHI on the basis that such disclosure is required by law without notifying CE so that CE shall have an opportunity to object to the disclosure and to seek appropriate relief. If CE objects to such disclosure, BA shall refrain from disclosing the PHI until CE has exhausted all alternatives for relief. BA shall require reasonable assurances from persons receiving PHI in accordance with Section 3.b. hereof that such persons will provide CE with similar notice and opportunity to object before disclosing PHI on the basis that such disclosure is required by law.

c. *Additional Restrictions.* If CE notifies BA that CE has agreed to be bound by additional restrictions on the uses or disclosures of CE's PHI pursuant to HIPAA or the HIPAA Regulations, BA shall be bound by such additional restrictions and shall not disclose CE's PHI in violation of such additional restrictions.

5. **Safeguards, Reporting, Mitigation and Enforcement.**

a. *Safeguards.* BA shall use any and all appropriate administrative, physical and technical safeguards to (i) prevent use or disclosure of CE's PHI otherwise than as provided by this Agreement, and (ii) protect the confidentiality, integrity and availability of any electronic PHI.

b. *BA's Agents.* BA shall not disclose PHI to any agent or subcontractor of BA except with the prior written consent of CE. BA shall ensure that any agents, including subcontractors, to whom it provides PHI, agree in writing to be bound by the same restrictions and conditions that apply to BA with respect to such PHI; provided, however, that BA shall not disclose or provide access to CE's PHI to any subcontractor or agent without the prior consent of CE.

c. *Reporting.* BA shall report to CE [as soon as practicable] [within] of BA becoming aware of any use or disclosure of CE's PHI in violation of this Agreement or applicable law. BA shall also report to CE within the same time-frame any Security Incident of which it becomes aware [OPTIONS INCLUDE] [as soon as reasonably practicable][within].

d. *Mitigation.* BA shall have procedures in place to mitigate, to the maximum extent practicable, any deleterious effect from any use or disclosure of CE's PHI in violation of this Agreement or applicable law.

e. *Sanctions.* BA shall have and apply appropriate sanctions against any employee, subcontractor or agent who uses or discloses CE's PHI in violation of this Agreement or applicable law.

f. *CE's Rights of Access and Inspection.* From time to time upon reasonable notice, or upon a reasonable determination by CE that BA has breached this Agreement, CE may inspect the facilities, systems, books and records of BA to monitor compliance with this Agreement. The fact that CE inspects, or fails to inspect, or has the right to inspect, BA's facilities, systems and procedures does not relieve BA of its responsibility to comply with this Agreement, nor does CE's (1) failure to detect or (2) detection of, but failure to notify BA or require BA's remediation of, any unsatisfactory practices constitute acceptance of such practice or a waiver of CE's enforcement or termination rights under this Agreement. The parties' respective rights and obligations under this Section 5.f. shall survive termination of the Agreement.

g. *United States Department of Health and Human Services.* BA shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of the United States Department of Health and Human Services ("HHS") for purposes of determining CE's compliance with HIPAA and the HIPAA Regulations; provided, however, that BA shall immediately notify CE upon receipt by BA of any such request for access by the Secretary of HHS, and shall provide CE with a copy thereof as well as a copy of all materials disclosed pursuant thereto. The parties' respective rights and obligations under this Section 5.g. shall survive termination of the Agreement.

6. Obligation to Provide Access, Amendment and Accounting of PHI.

a. *Access to PHI.* BA shall make available to CE such information as CE may require to fulfill CE's obligations to provide access to, and copies of, PHI in accordance with HIPAA and the HIPAA Regulations.

b. *Amendment of PHI.* BA shall make available to CE such information as CE may require to fulfill CE's obligations to amend PHI in accordance with HIPAA and the HIPAA Regulations. In addition, BA shall, as directed by CE, incorporate any amendments to CE's PHI into copies of such information maintained by BA.

c. *Accounting of Disclosures of PHI.* BA shall make available to CE such information as CE may require to fulfill CE's obligations to provide an accounting of disclosures with respect to PHI in accordance with HIPAA and the HIPAA Regulations. In addition, BA shall maintain a record of all disclosures of PHI, including the date of the disclosure, the name and, if known, the address of the recipient of the PHI, a brief description of the PHI disclosed, and the purpose of the disclosure which includes an explanation of the basis for such disclosure. BA shall make this record available to CE upon CE's request.

d. *Forwarding Requests From Individual.* In the event that any individual requests access to, amendment of, or accounting of PHI directly from BA, BA shall within two (2) days forward such request to CE. CE shall have the responsibility of responding to forwarded requests. However, if forwarding the individual's request to CE would cause CE or BA to violate HIPAA or the HIPAA Regulations, BA shall instead respond to the individual's request as required by such law and notify CE of such response as soon as practicable.

7. **Material Breach, Enforcement and Termination.**

a. *Term.* This Agreement shall be effective as of the Agreement Effective Date, and shall continue until the Agreement is terminated in accordance with the provisions of Section 7.b. [or the Agreement between the parties terminates]

b. *Termination.* CE may terminate this Agreement:

(1) immediately if BA is named as a defendant in a criminal proceeding for a violation of HIPAA or the HIPAA Regulations;

(2) immediately if a finding or stipulation that BA has violated any standard or requirement of HIPAA or other security or privacy laws is made in any administrative or civil proceeding in which BA has been joined; or

(3) pursuant to Sections 7.c. or 8.b. of this Agreement.

c. *Remedies.* If CE determines that BA has breached or violated a material term of this Agreement, CE may, at its option, pursue any and all of the following remedies:

(1) exercise any of its rights of access and inspection under Section 5.f. of this Agreement;

(2) take any other reasonable steps that CE, in its sole discretion, shall deem necessary to cure such breach or end such violation; and/or

(3) terminate this Agreement immediately.

d. *Knowledge of Non-Compliance.* Any non-compliance by BA with this Agreement or with HIPAA or the HIPAA Regulations automatically will be considered a breach or violation of a material term of this Agreement if BA knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance.

e. *Reporting to United States Department of Health and Human Services.* If CE's efforts to cure any breach or end any violation are unsuccessful, and if termination of this Agreement is not feasible, CE shall report BA's breach or violation to the Secretary of HHS, and BA agrees that it shall not have or make any claim(s), whether at law, in equity, or under this Agreement, against CE with respect to such report(s).

f. *Return or Destruction of Records.* Upon termination of this Agreement for any reason, BA shall return or destroy, as specified by CE, all PHI that BA still maintains in any form, and shall retain no copies of such PHI. If CE, in its sole discretion, requires that BA destroy any or all PHI, BA shall certify to CE that the PHI has been destroyed. If return or destruction is not feasible, BA shall inform CE of the reason it is not feasible and shall continue to extend the protections of this Agreement to such information and limit further use and disclosure of such PHI to those purposes that make the return or destruction of such PHI infeasible.

g. *Injunctions.* CE and BA agree that any violation of the provisions of this Agreement may cause irreparable harm to CE. Accordingly, in addition to any other remedies available to CE at law, in equity, or under this Agreement, in the event of any violation by BA of any of the provisions of this Agreement, or any explicit threat thereof, CE shall be entitled to an injunction or other decree of specific performance with respect to such violation or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages. The parties' respective rights and obligations under this Section 7.g. shall survive termination of the Agreement.

h. *Indemnification.* BA shall indemnify, hold harmless and defend CE from and against any and all claims, losses, liabilities, costs and other expenses resulting from, or relating to, the acts or omissions of BA in connection with the representations, duties and obligations of BA under this Agreement. The parties' respective rights and obligations under this Section 7.h. shall survive termination of the Agreement.

8. **Miscellaneous Terms.**

a. *State Law.* Nothing in this Agreement shall be construed to require BA to use or disclose PHI without a written authorization from an individual who is a subject of the PHI, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure.

b. *Amendment.* CE and BA agree that amendment of this Agreement may be required to ensure that CE and BA comply with changes in state and federal laws and regulations relating to the privacy, security, and confidentiality of PHI. CE may terminate this Agreement upon [] days written notice in the event that BA does not promptly enter into an amendment that CE, in its sole discretion, deems sufficient to ensure that CE will be able to comply with such laws and regulations. This Agreement may not otherwise be amended except by written agreement between the parties.

c. *No Third Party Beneficiaries.* Nothing express or implied in this Agreement is intended or shall be deemed to confer upon any person other than CE and BA, and their respective successors and assigns, any rights, obligations, remedies or liabilities.

d. *Ambiguities.* The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with applicable law protecting the privacy, security and confidentiality of PHI, including, but not limited to, HIPAA and the HIPAA Regulations.

e. *Primacy.* To the extent that any provisions of this Agreement conflict with the provisions of any other agreement or understanding between the parties, this Agreement shall control with respect to the subject matter of this Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Agreement Effective Date.

Name of CE

Name of BA

Signature of Authorized Representative

Signature of Authorized Representative

Name of Authorized Representative

Name of Authorized Representative

Title of Authorized Representative

Title of Authorized Representative