

BUSINESS ASSOCIATE AGREEMENT

1. DEFINITIONS

The terms set forth below as used in this Agreement shall have the following meanings:

1.1. **ADMINISTRATIVE SAFEGUARDS** shall mean administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the Covered Entity's workforce in relation to the protection of that Information.

1.2. **BUSINESS ASSOCIATE** shall refer to CareEntrust and shall have the same meaning as the term "Business Associate" as defined in 45 CFR § 160.103.

1.3. **COVERED ENTITY** shall refer to you, the User. Data is being furnished by Covered Entity to Business Associate for population-based activities relating to improving health and reducing health care costs, and care coordination.

1.4. **DATA AGGREGATION SERVICES** shall mean, with respect to Protected Health Information created or received by Business Associate in its capacity as a Business Associate of Covered Entity, the combining of such Protected Health Information by the Business Associate with the protected health information received by the Business Associate 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, as defined in 45 CFR § 164.501 and as such term may be amended from time to time in this cited regulation.

1.5. **DESIGNATED RECORD SET** shall mean a group of records maintained by or for Covered Entity that consists of the following: (a) medical records and billing records about Individuals maintained by or for a health care provider; (b) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (c) used in whole or in part, by or for Covered Entity to make decisions about Individuals. For these purposes, the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for Covered Entity.

1.6. **ELECTRONIC PROTECTED HEALTH INFORMATION** shall mean Individually Identifiable Health Information that is transmitted by Electronic Media or maintained in any medium described in the definition of Electronic Media in 45 CFR 160.103.

1.7. **ELECTRONIC TRANSACTIONS STANDARDS** shall mean the Standards for Electronic Transactions at 45 CFR Parts 160 and 162.

1.8. **HHS** shall mean the United States Department of Health and Human Services.

1.9. **INDIVIDUAL** shall mean the person who is the subject of the PHI, and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

1.10. **INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION** means that subset of health information, including demographic information collected from an individual, that:

- a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

- b. 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
 - 1. That identifies the individual; or
 - 2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

1.11. **PARTIES** shall mean Business Associate and Covered Entity.

1.12. **PHYSICAL SAFEGUARDS** shall mean the physical measures, policies, and procedures to protect Covered Entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

1.13. **PRIVACY RULE** shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164.

1.14. **PROTECTED HEALTH INFORMATION** ("PHI") shall have the same meaning as the term "protected health information" in 45 CFR § 160.301, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

1.15. **REQUIRED BY LAW** shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

1.16. **SECRETARY** shall mean the Secretary of the Department of Health and Human Services ("HHS") or his or her designee.

1.17. **SECURITY INCIDENT** shall mean the attempted and successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

1.18. **SECURITY RULE** shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 164, Subparts A and C.

1.19. **TECHNICAL SAFEGUARDS** shall mean the technology and the policy and procedures for its use that protected Electronic Protected Health Information and control access to it.

1.20. **OTHER TERMS AND AMENDMENTS TO TERMS:** Other capitalized terms shall have the meaning ascribed to them elsewhere in this Agreement, or, if no such definition is specified herein, shall have the same meaning as those terms in 45 CFR §§ 160.103, 164.304 and 164.501. Any reference to any Part, Subpart or section in the Code of Federal Regulations ("CFR") shall include any regulation issued thereunder regardless of the date of issue and shall include amendments made to such regulations regardless of the date of amendment.

2. **OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE**

2.1. **Limited Use and Disclosure of PHI:** Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.

2.2. **Safeguards Required:** Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

2.3. **Duty to Mitigate:** Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement and to cooperate with Covered Entity in its mitigation attempts.

2.4. **Duty to Report:** Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

2.5. **Duty to Ensure Agent or Subcontractor Compiles with Agreement:** Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

2.6. **Duty to Provide Access as Directed by Covered Entity:** Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner as specified by the Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524.

2.7. **Duty to Make Amendments as Directed by Covered Entity:** Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity, and in the time and manner specified by the Covered Entity.

2.8. **Duty to Make Internal Practices, Books, Records, Policies, and Procedures Available:** Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary, in a time and manner or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

2.9. **Duty to Record Disclosures:** Business Associate agrees to document such disclosures of Protected Health Information 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 Protected Health Information in accordance with 45 CFR 164.528.

2.10. **Duty to Provide Record of Disclosures to Covered Entity:** Business Associate agrees to provide to Covered Entity or an Individual, in time and manner specified by the Covered Entity, information collected in accordance with Section (i) immediately above, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

2.11. **Security Rule Requirements:**

a. **Safeguards to be in Place:** Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as provided for by this Agreement. Additionally, Business Associate shall

implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule.

- b. **Duty to Report to Covered Entity:** Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement or the Privacy Rule of which it becomes aware to include any Security Incident of which it becomes aware under the Security Rule. Accordingly, the Business Associate agrees to report any successful Security Incident of which it becomes aware to Covered Entity immediately, but not later than five (5) calendar days after the Security Incident. Further, the Business Associate agrees to report any attempted Security Incident of which it becomes aware to Covered Entity in the time, method, and manner identified by Covered Entity. In addition, Business Associate agrees to provide detailed information regarding any Security Incident(s) to Covered Entity upon request, within the capabilities of Business Associate. All reports provided by Business Associate pursuant to this Section shall include the actions and the mitigation steps, if any, taken by Business Associate in response to the Security Incident(s).
- c. **Duty for Business Associate's Agents, Subcontractors and Others:** Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created and received by Business Associate on behalf of, Covered Entity agrees to the same restrictions and conditions that apply throughout this Agreement to Business Associate with respect to such information to include, without limitation, the implementation of reasonable and appropriate safeguards to protect Electronic Protected Health Information. Such assurances shall be in writing and obtained prior to any disclosure of Electronic Protected Health Information from Business Associate to Business Associate's Agents, Subcontractors and/or Others.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

3.1. **Specific purposes:** Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity: to receive information from Covered Entity for internal use and to combine such data with information received from other covered entities to create community electronic health records for Individuals.

3.2. **Disclosure for Business Associate Management and Administration:** Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and 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 in which the confidentiality of the information has been breached.

3.3. **Data Aggregation Permitted:** Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

3.4. **Reporting of Violation Permitted:** Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with Sec. 164.502(j)(1).

4. OBLIGATIONS OF COVERED ENTITY

4.1. **Covered Entity to provide Notice of Privacy Practices:** Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

4.2. **Covered Entity to Notify Business Associate of Individual's Revocation of Permission:** Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

4.3. **Covered Entity to Notify Business Associate of Restriction:** Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information Permissible Requests by Covered Entity.

4.4. **Only Lawful Uses and Disclosures Allowed:** Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

5. TERM AND TERMINATION

5.1. **Term:** The Term of this Agreement shall terminate when all of the Protected Health Information 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 Protected Health Information, protections are extended to such information, in accordance with the provisions in Section 5.3.b below.

5.2. **Termination for Cause:** Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

- a. Provide an opportunity for Business Associate to cure the breach or end the violation within 30 calendar days or written notice by Covered Entity, and terminate this Agreement if Business Associate does not cure the breach or end the violation within the such period;
- b. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or
- c. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

5.3. **Effect of Termination.**

- a. Except as provided in Section 5.3.b below, upon termination of this Agreement for any reason, Business Associate shall return or destroy all Protected Health

Information received from, or created or received by Business Associate on behalf of, Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

- b. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon determination that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

6. MISCELLANEOUS

6.1. **Regulatory References:** A reference in this Agreement to a section in the Privacy Rule and/or the Security Rule means the section as in effect or as amended.

6.2. **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 to comply with the requirements of the Privacy Rule, the Security Rule, and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

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

6.4. **Interpretation:** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule and/or the Security Rule.