

Business Associate Agreement

A. **Definitions:** Terms used but not otherwise defined in this section shall have the same meaning as those terms in the HIPAA Privacy Rule.

- (1) Business Associate: shall mean Consultant/Vendor.
- (2) Covered Entity: shall mean City of Cedar Rapids
- (3) Designated Record Set: shall mean any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for Covered Entity.
- (4) Individual: shall mean the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with the Privacy Rule.
- (5) Privacy Rule: shall mean the Standards for Privacy of Individually Identifiable
 - a. Health Information at 45 CFR part 160 and part 164, subparts A and E.
- (6) Security Rule: shall mean the regulations at 45 CFR Part 160 and Part 164 that require the health plan to implement administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic health information that it creates, maintains, receives or transmits.
- (7) Protected Health Information ("PHI"): shall mean all individually identifiable health information transmitted or maintained by a covered entity, regardless of form, as the term is defined in 45 CFR 164.501. PHI for the purposes of this Agreement is limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- (8) Required By Law: shall mean a mandate contained in law that compels a covered entity to make a use or disclosure of PHI and that is enforceable in a court of law.
- (9) Security Incident: has meaning given to that term by 45 CFR 164.304.

B. Obligations and Activities of Business Associate

- (1) Business Associate agrees not to use or disclose PHI other than as permitted or required by this Agreement or as required by law. If Business Associate believes it is Required By Law or by a subpoena or court order to disclose any PHI, then Business Associate, prior to any disclosure, shall promptly notify Covered Entity in writing attaching a copy of the subpoena, court order, or other demand and shall make all reasonable efforts to allow Covered Entity an opportunity to seek a protective order or other judicial relief.
- (2) Business Associate agrees to use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of PHI other than as provided for by this Agreement;
- (3) 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 Agreement.
- (4) Business Associate agrees to promptly report to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which the Business Associate becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

- (5) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any agent, including a subcontractor that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions and requirements that apply to the business associate with respect to such information;
- (6) With respect to PHI contained in a Designated Record Set, Business Associate agrees to provide access, within seven (7) days of the request of Covered Entity, to such PHI to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements of the Privacy Rule. With respect to PHI contained in a Designated Record Set, Business Associate agrees to promptly make any amendment(s) to such PHI that Covered Entity directs.
- (7) Business Associate agrees to make all PHI, and internal practices, books, and records, including policies and procedures relating to the use and disclosure of PHI, available to the Covered Entity or to the Secretary of the Department of Health and Human Services ("Secretary"), upon request or at the direction of Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- (8) 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 for purposes other than treatment, payment, or health care operations, as per 45 CFR 164.528, and to provide the information contained in such documentation to Covered entity or to the Individual requesting the accounting within seven (7) days after a request for such information.
- (9) Business Associate will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic protected health information that it creates, receives, maintains or transmits on behalf of the Health Plan as required by the Security Rule. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides electronic protected health information, agrees to implement reasonable and appropriate standards to protect it.
- (10) Business Associate agrees to report to the Health Plan any security incident of which it becomes aware.

C. Permitted Uses and Disclosures by Business Associate

- (1) Except as otherwise limited in this Agreement, Business Associate may only use or disclose PHI to perform functions, activities, or services for, or on behalf of, the Covered Entity as specified in this Agreement, or in accordance with the written directions of the Covered Entity, provided that such use or disclosure would not violate the Privacy Rule if done by the Covered Entity or the minimum necessary policies and procedures of the Covered Entity.
- (2) Except as otherwise limited in this Agreement, Business Associate may use PHI for its proper management and administration or to carry out its legal responsibilities, provided that in the case of any disclosures for such purposes that are not Required by Law, Business Associate shall obtain reasonable assurances from the person to whom the disclosure is made that it will remain confidential and used and disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person agrees to notify Business Associate of any instances of which it becomes aware in which the confidentiality of PHI has been breached.
- (3) Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by the Privacy Rule.

D. Obligations of Covered Entity

- (1) Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices of Covered Entity to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- (2) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclosure of PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- (3) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to for an Individual to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

E. Termination and Survivability

- (1) The term of this Agreement shall be effective as of [Insert effective date}, and shall terminate on {Insert termination date or event} or on the date covered entity terminates for cause as authorized in paragraph (2) of this Section, whichever is sooner.
- (2) Upon Covered Entity's knowledge of a material breach by Business Associate of this Section ("Obligations of Business Associate"), Covered Entity shall either:
 - a. Provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity; or
 - b. Immediately terminate this Agreement if Business Associate has breached a material term of this Section ("Obligations of Business Associate") and cure is not possible; or
 - c. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary of the Department of Human Services.
- (3) Business Associate shall upon request of Covered Entity or upon termination for any reason of this Agreement, return to Covered Entity or destroy all PHI, including copies, abstractions, and compilations thereof, received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall not retain any copies of the PHI.
- (4) In the event Business Associate determines that returning or destroying PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. If Covered Entity agrees that return or destruction of PHI is infeasible, 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 the Business Associate maintains such PHI.
- (5) The obligations of business associate under this Section shall survive the termination of this agreement.

F. Miscellaneous

- (1) Regulatory References in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.
- (2) The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPA Rules and any other applicable law.
- (3) Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.