

HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“BAA”) is by and between _____ (the “Business Associate”) and **Family Health Initiatives** (the “Covered Entity”) and is effective as of _____ (the “Effective Date”).

WHEREAS, Covered Entity and Business Associate have entered into a Data Exchange Agreement (“Exchange Agreement”) which may involve the use or disclosure of Protected Health Information (defined below);

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and security of PHI received by or disclosed to Business Associate in compliance with the American Recovery and Reinvestment Act of 2009 and regulations issued under this Act (together the “ARRA”) and the Standards for Privacy of Individually Identifiable Health Information (the “Privacy Standards”) and the Standards for the Security of Electronic Protected Health Information (the “Security Standards”) under the Health Insurance Portability and Accountability Act of 1996, as amended from time to time (“HIPAA”);

WHEREAS, Covered Entity and Business Associate agree that this BAA sets forth the terms and conditions pursuant to which Protected Health Information that is provided by, or created or received by, Business Associate from or on behalf of Covered Entity, will be handled between Business Associate and Covered Entity during the term of BAA and after its termination.

NOW, THEREFORE, in consideration of the mutual covenants and promises set forth in the Agreement and below, the parties hereby agree as follows:

1. Definitions.

“Designated Record Set” (45 C.F.R. § 164.501) means a group of records maintained by or for a covered entity that is (i) the medical records and billing records about individuals maintained by or for a covered health care provider; or (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for a covered entity to make decisions about individuals.

“Electronic Protected Health Information” or “EPHI” (45 C.F.R. § 160.103) means individually identifiable health information transmitted by Electronic Media or maintained in Electronic Media.

“Electronic Media” (45 C.F.R. § 160.103) means (1) electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as a magnetic tape or disk, optical disk, or digital memory card; or (2) transmission media used to exchange information already in electronic storage media.

Transmission media include, for example, the internet (wide open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.

“Exchange Agreement” means the agreement executed between Business Associate and Covered Entity dated _____.

“Individual” (45 C.F.R. § 160.103) means the person who is the subject of Protected Health Information.

“Individually Identifiable Health Information” (45 C.F.R. § 160.103) means information, including demographic information, collected from an individual and (i) is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and (ii) relates to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual; and (a) 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.

“Protected Health Information (PHI)” (45 C.F.R. § 160.103) means Individually Identifiable Health Information that is (i) transmitted by electronic media; (ii) maintained in any medium constituting electronic media; or (iii) transmitted or maintained in any other form or medium.

“Security Breach” (as defined under the ARRA, including certain exceptions) means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information.

“Security Incident” (45 C.F.R. § 164.304) means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

2. Use and Disclosure of PHI. Business Associate may use and disclose PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity only as permitted or required by the Exchange Agreement, this BAA, or as otherwise permitted or required by law.

To the extent Business Associate is to carry out one or more of the 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. All such uses and disclosures also shall be in compliance with each applicable requirement of 45 C.F.R. § 164.504(e). Business Associate shall not, and shall ensure that its directors, officers, employees, contractors, and agents, including subcontractors, do not use or disclose PHI received from Covered Entity or created or received by Business Associate on

behalf of Covered Entity in any manner that would constitute a violation of the Privacy Standards if used in such manner by Covered Entity. Except as otherwise limited in this BAA, Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are Required by Law (as defined under 45 C.F.R. § 164.103), 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. Except as otherwise limited in this BAA, Business Associate may use PHI to provide data aggregation services to the Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B). Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI unless Business Associate or Covered Entity has obtained a valid HIPAA-compliant authorization from the individual that specifies whether the PHI can be further exchanged for remuneration by Business Associate.

3. Safeguards. Business Associate agrees that it will use appropriate administrative, technical and physical safeguards to prevent use and/or disclosure of PHI otherwise than as provided for under this BAA. Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, maintains, or transmits on behalf of the Covered Entity, as required by the Security Standards and the ARRA, including without limitation, 45 C.F.R. §§ 164.308, 164.310, and 164.312. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides such information agrees in writing to implement reasonable and appropriate safeguards to protect it.

4. Policies and Procedures. Business Associate agrees to implement reasonable and appropriate policies and procedures to comply with the Security Standards as required by the ARRA. Business Associate also agrees to maintain such policies and procedures in written or electronic form, and will document and retain such documentation regarding all actions, activities and assessments required under the Security Standards consistent with the ARRA and 45 C.F.R. § 164.316(b).

5. Training. Business Associate agrees that all members of Business Associate's workforce who will use or disclose Covered Entity's PHI will: (a) be trained (in accordance with 45 C.F.R. § 164.308(5)) concerning Business Associate's HIPAA Privacy and Security policies and practices and compliance with the Privacy and Security Standards and the ARRA; and (b) agree in writing to abide by such policies and practices.

6. 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.

7. Reporting of Disclosures of PHI. Business Associate shall report to Covered Entity within forty-eight (48) hours any Security Incident, Security Breach or use or disclosure of PHI in violation of this BAA of which it becomes aware. A Security Breach/Incident will be considered “discovered” by Business Associate as of the first day on which such Breach/Security Incident is known to Business Associate (including any person, other than the individual committing the Breach/Incident, that is an employee, officer, or other agent of Business Associate), or should reasonably have been known to Business Associate to have occurred. Business Associate’s initial reports to Covered Entity regarding Security Breaches/Incidents shall include the identification of each Individual whose unsecured PHI (as defined under ARRA and the HIPAA Standards) has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach/Incident, the type of PHI accessed, acquired or disclosed, as well as any other information required by law. Business Associate shall take prompt corrective action to cure any deficiencies and will take any action pertaining to such Security Breach/Incident required by applicable federal and state laws and regulations and as directed by Covered Entity. Business Associate will provide a written report to Covered Entity within ten (10) calendar days of the discovery of any use or disclosure of Covered Entity’s PHI not permitted by this Agreement, and such report shall describe in detail: (i) the actions taken by Business Associate to mitigate any harmful effect of the unauthorized use or disclosures and (ii) what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure. To the extent Business Associate coordinates and assists Covered Entity in providing notice of the Security Breach/Security Incident to Individuals, Business Associate agrees to do so in accordance with the ARRA, including, without limitation, ARRA provisions regarding timeliness, content, and recipients of such notice.

8. Agreements with Third Parties. Business Associate agrees to require any agent or subcontractor to whom it provides PHI to agree in writing to be bound by the same restrictions and conditions that apply through this BAA to Business Associate with respect to such PHI. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate safeguards to protect the EPHI. Business Associate shall disclose to such subcontractors or agents only the minimum PHI necessary (as defined under the HIPAA Standards and the ARRA) to perform or fulfill a specific function required or permitted under the HIE Agreement or this BAA.

9. Access to Information. Business Associate agrees to provide access, at the request of Covered Entity or an Individual, to PHI in a Designated Record Set to the Individual or Covered Entity so that Covered Entity may meet the requirements of 45 C.F.R. § 164.524 and the ARRA (including access to the information in electronic format as required under the ARRA).

10. Amendments/Availability of PHI for Amendment. Business Associate agrees to make any amendments to PHI in a Designated Record Set that the Covered Entity directs in accordance with the requirements of 45 C.F.R. § 164.526.

11. Accounting of Disclosures. Business Associate agrees to document such disclosures of PHI and information related to such disclosures, and retain such documentation

and information, as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and the ARRA. Business Associate agrees to respond to requests from Covered Entity or an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and the ARRA. As required under the ARRA, Business Associate agrees to respond to Individual requests for accountings relating to electronic health records if Covered Entity includes Business Associate on a list of business associates who may respond on Covered Entity's behalf.

12. Restrictions. Unless otherwise prohibited by law, Business Associate agrees to respond to requests by an Individual for restrictions on the use and disclosure of PHI in accordance with 45 C.F.R. § 164.522 (or implement a restriction agreed to by Covered Entity), including requests for confidential communications, and to notify Covered Entity immediately regarding any restrictions to which Business Associate agrees. Business Associate also agrees to comply with a request for a restriction if the disclosure is to a health plan for the purposes of carrying out payment or health care operations (and is not for treatment) and the PHI pertains solely to a healthcare item or services for which the health care provider involved has been paid out of pocket in full.

13. Availability of Books and Records. Business Associate hereby agrees to make its internal policies, procedures, practices, books, records and agreements relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary of the Department of Health and Human Services (the "Secretary") for purposes of determining Covered Entity's compliance with the Privacy and Security Standards and the ARRA.

14. Return of PHI upon Termination. Upon termination of the Exchange Agreement or this BAA for any reason, Business Associate shall return all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity and which Business Associate still maintains in any form. Prior to doing so, Business Associate further agrees to recover any PHI in the possession of its subcontractors or agents. Business Associate shall not retain any copies of such PHI. If it is not feasible to return such PHI, Business Associate agrees to extend any and all protections, limitations, and restrictions in this BAA to the Business Associate's use and disclosure of any PHI retained after the termination of the BAA, and to limit any further uses and disclosures to the purpose or purposes that make the return of PHI infeasible. If it is not feasible for Business Associate to obtain from a subcontractor or agent any PHI in the possession of the subcontractor or agent, Business Associate must require the subcontractor and/or agent to agree in writing to extend any and all protections, limitations, and restrictions in this BAA to the subcontractors' and/or agents' use and disclosure of any PHI retained after the termination of the BAA, and to limit any further uses and disclosures to the purposes that make the return of the PHI infeasible. This Section shall survive termination or expiration of this BAA for whatever reason.

15. Term and Termination. This BAA shall be effective as of the Effective Date and shall continue in effect for so long as Business Associate is a Business Associate of Covered

Entity, or as otherwise terminated as provided herein. Covered Entity may immediately terminate the Exchange Agreement and this BAA and any related agreements if Covered Entity determines that Business Associate has breached a material term of this BAA. Alternatively, Covered Entity may (i) provide Business Associate with thirty (30) days written notice of the existence of an alleged material breach; and (ii) afford Business Associate an opportunity to cure said alleged material breach to Covered Entity's satisfaction within the stated time period. Failure to cure the alleged breach to Covered Entity's satisfaction within such time period is grounds for immediate termination of the BAA; provided, however, that in the event that Covered Entity determines that termination of the BAA is not feasible, Business Associate hereby acknowledges that Covered Entity shall have the right to report the breach to the Secretary, notwithstanding any other provision of the BAA to the contrary. To the extent that Business Associate knows of a pattern of activity or practice of Covered Entity that constitutes a material breach or violation of Covered Entity's obligations under this BAA, Business Associate will take reasonable steps to assist Covered Entity in curing the breach or ending the violation, and if such steps are unsuccessful, Business Associate may terminate this BAA and the Exchange Agreement, if feasible. If termination is not feasible, Business Associate may report the problem to the Secretary.

16. No Third Party Beneficiaries. Nothing in the BAA shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

17. Covered Entity's Obligations. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI. 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 Associate's use or disclosure of PHI. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

18. Regulatory References. A reference in the BAA to a section in the Privacy or Security Standards and the ARRA means the section as in effect or as amended from time to time.

19. Amendment. No changes, amendments, or alterations of this BAA shall be effective unless signed by duly authorized representatives of both parties, except as expressly provided herein. The parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the Privacy or Security Standards, the ARRA, or other applicable law.

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

FAMILY HEALTH INITIATIVES

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____