

HIPAA Business Agreement

The following HIPAA Business Associate Agreement (the "Agreement") is entered into by the parties on the dates indicated below their respective signature lines but is effective as of _____, 20__ ("Effective Date") by and between _____ ("Covered Entity") and _____. ("Business Associate").

WHEREAS, Business Associates may work on behalf of Covered Entities by maintaining, transmitting, creating, or receiving Protected Health Information (as defined in 45 CFR 160.103);

WHEREAS, Covered Entity may be required to comply with 42 U.S.C. 1320d et seq. enacted by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") and the implementing regulations set forth at 45 CFR Parts 160, 162 and 164 ("HIPAA Regulations"). Herein, "PHI" means Protected Health Information maintained, transmitted, created, or received by a Business Associate on behalf of or from a Covered Entity.

WHEREAS, Business Associates may be directly subject to HIPAA, HITECH, HIPAA Regulations, and applicable state law in accordance with the HIPAA Regulations and applicable state law.

NOW, THEREFORE, the parties agree as follows:

1. PHI may only be used or disclosed in accordance with this Agreement or as required by law. Business Associate may use or disclose PHI as required to perform *[use the following if a written service agreement exists: The parties are obligated to perform certain services as described in the Service Agreement ("Services") as described in the Service Agreement. In the absence of a written service agreement, use the following method: the following services on behalf of Covered Entity: _____ (the "Services")]*, provided that Business Associate does not use or disclose PHI in a manner that would violate HIPAA Regulations if done by Covered Entity. Under HIPAA Regulations, HITECH, and applicable state law, Business Associates are prohibited from using, selling, or disclosing PHI for marketing or fundraising purposes. A Business Associate must limit its uses and disclosures of, as well as its requests for, PHI (i) when practical, to the information that makes up a limited data set (45 CFR 164.514); and (ii) in all other cases subject to the requirements of 45 CFR §164.502(b), to the minimum amount of PHI necessary to fulfill the purpose for which the PHI is being used, disclosed or requested. When the Covered Entity informs Business Associate of a restriction request limiting Business Associate's use or disclosure of PHI, Business Associate will comply. As a Business Associate, you are required to comply with the HIPAA Regulations that apply to Covered Entities.

2. To protect PHI from uses or disclosures not permitted under this Agreement, Business Associates agree to maintain reasonable and appropriate administrative, technical, and physical safeguards, including, but not limited to, developing policies and procedures to prevent, detect, or mitigate identity theft based on PHI or information derived from PHI. Furthermore, Business Associate is responsible for complying with the requirements of 45 CFR Part 164, subpart C, of the HIPAA Regulations and any guidance issued by the Secretary of the Department of Health and Human Services ("HHS"). To ensure the confidentiality, integrity and availability of

HIPAA Business Agreement

electronic PHI, Business Associate agrees to utilize multiple security mechanisms, including, but not limited to, authentication controls, authorization controls, audit controls, and encryption.

3. In the event Business Associate becomes aware of or discovers any violation of this Agreement, any Security Incident (as defined at 45 CFR §164.304), any Red Flag (as defined at 16 CFR §681.2(b)) related to any individual who is the subject of PHI, and any Breach of Unsecured Protected Health Information (both as defined at 45 CFR §164.402), the Business Associate shall promptly notify the Covered Entity of such use, disclosure, incident, Red Flag or breach.

Reports of breaches must be submitted within ten (10) business days of discovery by the Business Associate, and must include the information specified in 45 CFR 164.410. The Business Associate will mitigate any adverse effects known to it as a result of using or disclosing PHI that is not permitted by this Agreement, to the extent practicable. When a Breach occurs involving Business Associate, Business Associate shall promptly reimburse Covered Entity for any reasonable costs incurred by Covered Entity, including but not limited to printing, postage costs, and toll-free hotline costs.

4. In accordance with 45 CFR §§ 164.308(b)(2) and 164.502(e)(1)(i), It is the responsibility of Business Associate to ensure that all subcontractors and agents who create, receive, maintain, or transmit PHI on Business Associate's behalf are bound by the same restrictions, terms, and conditions that apply to Business Associate under this Agreement.

5. In accordance with 45 CFR §164.524 and within fifteen (15) days of a request by Covered Entity for access to PHI about an individual contained in a Designated Record Set (as defined at 45 CFR §164.501), Business Associate shall provide such information in the form requested by Covered Entity. It is Business Associate's responsibility to provide a copy of the requested PHI in the electronic format and form requested by the individual if it is readily producible, or, if not, in a readable electronic form and format as agreed to by Covered Entity and the individual. Whenever an individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within ten (10) days. Covered Entity is responsible for denying access to PHI.

6. In accordance with 45 CFR §164.526, and within fifteen (15) days of receiving a request from Covered Entity for the amendment of an individual's PHI in a Designated Record Set (for as long as the PHI is maintained in the Designated Record Set), the Business Associate shall provide the information to Covered Entity and incorporate the amendment into the PHI in accordance with 45 CFR §164.526. If an amendment request is delivered directly to Business Associate, Business Associate shall forward the request to Covered Entity within ten (10) days of receiving it.

7. As stipulated in 45 CFR 164.528 or regulations under HITECH, Business Associates are exempt from accounting obligations when they disclose PHI. In accordance with 45 CFR 164.528, Business Associates must record the information that covered entities are required to record for each disclosure. Business Associate shall provide the information required to be maintained pursuant to this Section 7 to the Covered Entity, or, if requested by the Covered Entity, to the individual when it receives a request for an accounting of disclosures of PHI. If the

HIPAA Business Agreement

request for an accounting is delivered directly to Business Associate, Business Associate shall forward the request to Covered Entity within ten (10) days.

8. In order to determine compliance with HIPAA regulations, Business Associate shall make available to HHS its internal practices, books, and records regarding the use and disclosure of PHI.

9. Business Associate may not use or disclose PHI in a manner that would violate HIPAA Regulations if done by the Covered Entity, provided that the Business Associate:

a. Manage, administer, and perform its legal duties using PHI.

b. In the event that PHI must be disclosed to manage and administer it properly and fulfill legal responsibilities, the Business Associate obtains reasonable assurances from the recipient that the PHI will remain confidential and will be used or further disclosed as required by law or for the purpose for which it was disclosed to the recipient, and the recipient informs the Business Associate about any breaches of confidentiality of the information.

c. Report violations of law to appropriate Federal and State authorities, in accordance with 45 CFR § 164.502(j)(1).

d. Using its capacity as a business associate to other covered entities, Business Associate may aggregate the PHI it possesses with the Protected Health Information of other covered entities that Business Associate has in its possession, provided that the aggregated data will provide Covered Entity with insights into its health care operations.

e. Create de-identified information from PHI if it meets the requirements of 45 CFR 164.514(b).

10. If Business Associate conducts standard transactions (as defined in 45 CFR Part 160) for or on behalf of Covered Entity, Business Associate will comply with the HIPAA Regulations and require each agent or contractor (including any subcontractor) involved in the conduct of such standard transactions to comply by written contract with each requirement (as outlined in 45 CFR Parts 160 and 162). In connection with standard transactions conducted for or on behalf of Covered Entity, Business Associate will not enter into, or permit its agents or contractors (including subcontractors) to enter into, any trading partner agreement that: (i) changes a data element or segment in a standard transaction, including its definition, data condition, or use; (ii) extends the maximum defined data set by adding data segments or elements; (iii) uses any code or data element that is marked "not used" or is not in the standard transaction's implementation specification; or (iv) alters the implementation specification in a way that changes its meaning or intent. In accordance with HIPAA Regulations, Business Associate agrees to participate in any test modifications conducted by Covered Entity.

11. ***[use the following if a written service agreement exists: The Agreement shall begin on the Effective Date and continue until terminated.*** A party may terminate this Agreement and the Service Agreement if it determines that the other party has breached a material provision of this Agreement and has failed to resolve the breach within thirty (30) days of being notified. This

HIPAA Business Agreement

Agreement and the Service Agreement may be terminated by the non-breaching party after written notice to the other party if a resolution cannot be reached. The non-breaching party is responsible for reporting the breach to HHS if there is no termination. A termination of this Agreement will constitute a default on the part of the Business Associate under the Service Agreement.

[use the following if there is NOT a written service agreement in place: The Agreement shall become effective on the Effective Date and continue until Business Associate ceases to provide the Services. If either party determines that the other party has breached a material provision of this Agreement and has not cured the breach within thirty (30) days after being notified of the breach, either party may terminate this Agreement immediately. Upon written notice to the other party, the non-breaching party may terminate this Agreement if a resolution is not possible. Non-breaching parties should report breaches to HHS if termination is not feasible. Upon termination of this Agreement, Business Associate will cease performing Services on behalf of the Covered Entity.]

12. In the event this Agreement is terminated, Business Associate shall either return or destroy all PHI that Business Associate still maintains, at no cost to Covered Entity. The Business Associate shall retain no copies of PHI. To the extent that it is not feasible to return or destroy such PHI, the terms and provisions of this Agreement will survive termination, and Business Associate shall only disclose or use such PHI for those purposes that prevent it from being returned or destroyed.

13. This Agreement does not create any rights or remedies for third parties or any agency relationship between the parties. Business Associate will be subject to the penalty provisions of HITECH if acting as Business Associate under HIPAA Regulations. A final regulation or amendment to a final regulation promulgated by HHS that affects PHI will automatically amend this Agreement so that the obligations imposed on the parties remain compliant. It is understood that the terms and conditions of this Agreement will override and govern all conflicting terms and conditions of any other agreement between the parties regarding the Services. ***[include the following if a written service agreement exists:*** including the Service Agreement], all of which remain in full force and effect.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement on the dates set forth below.

HIPAA Business Agreement

For Covered Entity

By: _____

Name: _____

Title: _____

Date: _____

For Business Associate

By: _____

Name: _____

Title: _____

Date: _____