

BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is entered into on the _____ day of _____, 20____, by and between

(hereinafter referred to as "Covered Entity") and

(hereinafter referred to as "Business Associate").

WHEREAS, Covered Entity has engaged Business Associate to perform certain services or provide certain goods, or both.

WHEREAS, Covered Entity possesses or will possess individually identifiable health information, which information is subject to the federal Health Insurance Portability and Accountability Act of 1996, the federal Health Information Technology for Economic and Clinical Health Act and all related regulations.

WHEREAS, in the course of performing services or providing goods to Covered Entity, Business Associate may receive individually identifiable health information from Covered Entity or otherwise obtain access to such information.

WHEREAS, Covered Entity seeks to ensure that Business Associate appropriately safeguards all such individually identifiable health information.

WHEREAS, Covered Entity is subject to the Red Flags Rule, a federal regulation promulgated by the Federal Trade Commission aimed at preventing identity theft.

WHEREAS, Covered Entity seeks to ensure that Business Associate adopts appropriate identity theft prevention methods.

WHEREAS, Covered Entity and Business Associate are subject to the federal False Claims Act, as amended by the Fraud Enforcement and Recovery Act of 2009.

WHEREAS, Covered Entity seeks to ensure that Business Associate is made aware of its rights and obligations under the False Claims Act.

NOW, THEREFORE, the parties hereby agree as follows:

1. DEFINITIONS

- a. "Breach" shall have the same meaning as the term "breach" in the Breach Notification Rule, defined below.

- b. "Breach Notification Rule" means the Breach Notification for Unsecured Protected Health Information, Interim Final Rule, published in the Federal Register on August 24, 2009.
- c. "False Claims Act" means the federal False Claims Act, 31 U.S.C. Section 3729, as amended by the Fraud Enforcement and Recovery Act of 2009, Public Law 111-21.
- d. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
- e. "HIPAA Privacy Rule" means regulations promulgated under HIPAA by the U.S. Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subpart E.
- f. "HIPAA Security Rule" means regulations promulgated under HIPAA by the U.S. Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subpart C.
- g. "HITECH" means the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009.
- h. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 C.F.R. §164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- i. "Red Flags Rule" means federal regulations promulgated by the Federal Trade Commission, including, but not limited to, 16 C.F.R. §681.2.
- j. "Unsecured PHI" shall have the same meaning as the term "unsecured protected health information" in the Breach Notification Rule.
- k. Any terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms have under HIPAA, HITECH, the HIPAA Privacy Rule, the HIPAA Security Rule and the Breach Notification Rule.

2. PERMITTED USES AND DISCLOSURES

- a. Business Associate may use and/or disclose PHI received from, or created or received on behalf of, Covered Entity to perform functions, activities or services for or on behalf of Covered Entity as set forth in a service agreement between Business Associate and Covered Entity or, in connection with any one or more of the following services to be performed on Covered Entity's behalf:

Please check where applicable:

_____ Billing, including claims processing or administration and benefit management

_____ Legal services

_____ Accounting, financial or actuarial services

_____ Other, please specify: _____

3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE UNDER HIPAA, HIPAA PRIVACY RULE, HIPAA SECURITY RULE, HITECH AND THE BREACH NOTIFICATION RULE

- a. Use or Disclosure. Business Associate shall not use or disclose PHI other than as permitted or required by this Agreement or as required by law. Business Associate shall comply with all provisions of HIPAA, HITECH, the HIPAA Privacy Rule and the HIPAA Security Rule that relate to the privacy and security of PHI and that are applicable to Covered Entity and Business Associate.
- b. Safeguards. Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as specifically provided for by this Agreement, including, without limitation, (i) implementing administrative, physical and technical safeguards to reasonably protect the privacy and security of PHI; and (ii) ensuring that any subcontractor or agent that receives PHI from Business Associate agrees to implement reasonable and appropriate safeguards to protect the privacy and security of PHI.
- c. Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Breach of Unsecured PHI or any use or disclosure of PHI by Business Associate that violates the requirements of this Agreement. Business Associate shall cooperate with and assist Covered Entity in any investigation and/or cure of a Breach of Unsecured PHI or other violation of this Agreement.
- d. Reporting. Business Associate shall report to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, as soon as reasonably practicable.
- e. Subcontractors and Agents. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply to Business Associate as a result of this

Agreement.

- f. **Access.** At the request of Covered Entity, Business Associate shall provide to Covered Entity (or to an individual) access to PHI contained in a designated record set in order to comply with the access provisions contained in 45 C.F.R. §164.524 and/or the policies of Covered Entity. Such access shall be provided by Business Associate in the time and manner designated by Covered Entity, including, where applicable, access by electronic means pursuant to HITECH Section 13405(e).
- g. **Amendment.** At the request of Covered Entity or an individual, Business Associate shall make any amendment(s) to PHI in a designated record set that the Covered Entity directs or agrees to pursuant to the amendment of records provisions in 45 C.F.R. §164.526 and/or the policies of Covered Entity. Such amendments shall be made by Business Associate in the time and manner designated by Covered Entity.
- h. **Audit and Inspection.** Business Associate shall make internal practices, books and records 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 Covered Entity or to the Secretary of the US Department of Health and Human Services (HHS), or his or her designee, for the purposes of the Secretary determining Covered Entity's compliance with the HIPAA Privacy Standards. Such information shall be made available in a time and manner designated by Covered Entity or the Secretary of HHS.
- i. **Documentation of Disclosures.** Business Associate shall document such disclosures of PHI, and such information related to such disclosures in order to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528, the policies of Covered Entity and HITECH Section 13405(c).
- j. **Accounting.** Business Associate shall provide to Covered Entity or to an individual information collected in accordance with Section 3(i) of this Agreement, to permit 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 HITECH Section 13405(c).
- k. **Breach Notification.** In the event of a Breach of Unsecured PHI maintained by Business Associate, Business Associate shall perform a risk assessment to determine if such Breach poses a significant risk of harm to the individual. If a significant risk of harm is determined to exist, Business Associate shall without unreasonable delay and no later than 60 days from the date of discovery of the Breach, provide all affected individuals with written notice of such Breach. Said notice shall be written in plain language and will contain the following information: (i) a brief description of what happened, the date of the Breach, if

known, and the date of discovery; (ii) the type of PHI involved in the Breach; (iii) any precautionary steps the individual should take; (iv) a description of what Business Associate is doing to investigate and mitigate the Breach and prevent future breaches; and (v) how the individual may contact Business Associate to discuss the Breach.

4. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE UNDER FALSE CLAIMS ACT

- a. Business Associate acknowledges and agrees that, as a participant in federal health care programs, Covered Entity is subject to the federal False Claims Act, as amended by the Federal Enforcement and Recovery Act of 2009. Business Associate further acknowledges and agrees that, as a consultant or contractor of Covered Entity, it is also subject to all rules and requirements contained in the False Claims Act, as amended by the Federal Enforcement and Recovery Act of 2009.
- b. Business Associate shall not knowingly (i) present or cause to be presented a false record or fraudulent claim for payment or approval or (ii) make, use or cause to be made or used, a false record or statement material to a false or fraudulent claim.
- c. Business Associate shall immediately notify Covered Entity if it becomes aware of any billing irregularities or any suspicious activity that may indicate fraud.
- d. Business Associate shall provide training to its management and employees on prevention of fraud and false claims activities.

5. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE UNDER RED FLAGS RULE

- a. Business Associate shall implement policies and procedures to identify, prevent and mitigate the risk of identity theft. Such policies and procedures will include:
 - i. provisions regarding the identification and detection of red flags relevant to Business Associate's business activities on behalf of Covered Entity;
 - ii. proper customer identification procedures; and
 - iii. procedures for the prevention and mitigation of identity theft.
- b. Business Associate shall provide training to its management and employees on identity theft prevention procedures and shall provide a copy of Business Associate's identity theft prevention policy to all management and employees.
- c. Business Associate shall notify Covered Entity of any suspicious activity that may indicate possible identity theft and take steps to prevent or mitigate such possible identity theft.

6. OBLIGATIONS OF COVERED ENTITY

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA, HITECH, the HIPAA Privacy Rule, the HIPAA Security Rule or the Breach Notification Rule, if done by Covered Entity. Further, Covered Entity shall not request Business Associate to make any acts or omissions that would not be permissible under the False Claims Act or the Red Flags Rule, if done by Covered Entity.

7. TERM AND TERMINATION

- a. Term. The term of this Agreement shall begin on the date first written above and shall continue until the Agreement is terminated in accordance with the provisions of Section 7(b) or 7(c) hereof, or when the underlying service agreement between the parties terminates.
- b. Termination by Covered Entity for Cause. Upon Covered Entity's knowledge of a material breach of the terms of this Agreement by Business Associate, Covered Entity may, in its sole discretion, either (i) provide Business Associate with notice of and an opportunity to cure such breach and then terminate this Agreement if Business Associate does not cure breach or end the violation within time period specified by Covered Entity, or (ii) terminate this Agreement immediately. If neither cure of the breach nor termination of the Agreement is feasible, Covered Entity shall notify the U.S. Department of Health and Human Services of the uncured breach.
- c. Termination by Business Associate for Cause. Upon Business Associate's knowledge of a material breach of the terms of this Agreement by Covered Entity, Business Associate shall provide Covered Entity with notice of and an opportunity to cure such breach and then terminate this Agreement if Covered Entity does not cure breach or end the violation within time period specified by Covered Entity. If neither cure of the breach nor termination of the Agreement is feasible, Business Associate shall notify the U.S. Department of Health and Human Services of the uncured breach.
- d. Effect of Termination.
 - (1) Upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI 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 retain no copies of the PHI.
 - (2) Notwithstanding the foregoing, in the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions

that make the return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of the 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 Business Associate maintains such PHI.

8. MISCELLANEOUS

- a. **Regulatory References.** A reference in this Agreement to a section of HIPAA, HITECH, the HIPAA Privacy Rule, the HIPAA Security Rule, the Breach Notification Rule, the Red Flags Rule or the False Claims Act means the section in effect or as amended.
- b. **Amendment.** The parties agree to take such action necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of any applicable statute, rule or regulation.
- c. **Survival.** The respective rights and obligations of the parties hereto under Section 7(d)(1) and 7(d)(2) of this Agreement shall survive the termination of this Agreement.
- d. **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with any applicable statute, rule or regulation.
- e. **State Law.** Nothing in this Agreement shall be construed to require Business Associate to use or disclose PHI without written authorization from the individual who is the subject of the PHI, or written authorization from any other person, where state law requires authorization for such use or disclosure.
- f. **Injunctions.** Covered Entity and Business Associate agree that any violation by Business Associate of any of the provisions of this Agreement may cause irreparable harm to Covered Entity. Accordingly, in addition to any other remedies available to Covered Entity at law, in equity or under this Agreement, Covered Entity shall be entitled to an injunction or other decree of specific performance with respect to any violation by Business Associate of any of the provisions of this Agreement, or any explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages.
- g. **Indemnification.** Business Associate shall indemnify, hold harmless and defend Covered Entity from and against any and all claims, losses, liabilities, costs and other expenses resulting from or relating to the acts or omissions of Business Associate in connection with the representations, duties and obligations of Business Associate under this Agreement.

- h. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended or shall be deemed to confer upon any person other than Covered Entity, Business Associate and their respective successors and assigns, any rights, obligations, remedies or liabilities.
- i. 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.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the date first written above.

Name of Covered Entity

Name of Business Associate

BY: _____
Signature of Authorized Representative

BY: _____
Signature of Authorized Representative

Name and Title

Name and Title