BUSINESS ASSOCIATE AGREEMENT

**THIS BUSINESS ASSOCIATE AGREEMENT (this “Agreement”)** is entered into effective \_\_\_\_\_\_\_\_\_ by and between \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(the “Covered Entity”) with an address at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_ , (the “Business Associate”), with an address at \_\_\_\_\_\_\_\_\_ (each a “Party” and collectively the “Parties”).

WITNESSETH

**WHEREAS**, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is considered a “Covered Entity” and \_\_\_\_\_\_\_\_\_ is considered a “Business Associate” as such terms are defined under the Health Insurance Portability and Accountability Act of 1996 (as amended, modified or superseded from time to time, “HIPAA”) and the final Privacy Rule issued pursuant thereto (codified at 45 CFR Parts 160 and 164 as amended, modified, or superseded from time to time, the “Privacy Rule”) (collectively, HIPAA, the Privacy Rule and any other state or federal legislation relating to the protection of health information is referred to herein as “Applicable Privacy Law”); and

**WHEREAS**, amendments to the HIPAA Regulations contained in the HIPAA Omnibus Final Rule became effective on March 26,2013, and amended HIPAA’s Privacy, Security, Breach Notification and Enforcement Rules: and

**WHEREAS**, The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

**WHEREAS,** Covered Entity will make available and/or transfer to Business Associate certain Protected Health Information, in conjunction with goods or services that are being provided by Business Associate to Covered Entity, that is confidential and must be afforded special treatment and protection;

**WHEREAS**, Covered Entity and Business Associate desire to enter into this Agreement in order to comply with the Applicable Privacy Law;

**THEREFORE**, in consideration of the Parties’ continuing obligations under the HIPAA Privacy Rule and Security Rule, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the provisions of this Agreement in order to address the requirements of the HIPAA Privacy Rule and Security Rule and to protect the interests of both Parties. In consideration of the mutual promises below and the exchange of information pursuant to this Agreement, Covered Entity and Business Associate agree as follows:

1. **Defined Terms**. Except as otherwise defined below or elsewhere in this Agreement, all capitalized terms shall have the meanings provided in 45 CFR 160.103 and 164.501. (For convenience, a few of the definitions are highlighted below.)

a. **Breach** shall have the same meaning as the term “breach” in 45 CFR 164.402.

b. **Business Associate** shall have the meaning given to such term in 45 C.F.R. § 160.103.

c. **CFR** shall mean Code of Federal Regulations.

d. **Agreement** shall refer to this entire document.

e. **Covered Entity** the term “Covered Entity” (abbreviated as “CE”) shall mean 1) a health plan; 2) a healthcare clearinghouse; 3) a healthcare provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

f. **Electronic Protected Health Information** shall have the same meaning as the term “electronic protected health information” in 45 CFR 160.103.

g. **HHS Privacy Regulations** shall mean the Code of Federal Regulations (CFR) at Title 45, Sections 160 and 164, Subparts A and E.

h. **HIPAA Data Breach Notification Rule** means 45 CFR Part 164, Subpart D and any amendments thereto.

i. **Individual** shall mean the person who is the subject of the Protected Health Information, and has the same meaning as the term “Individual” as defined by 45 CFR 160.103 and shall include a person who qualifies as a person who qualifies as a personal representative in accordance with 45 CFR 164.502.

j. **Parties** the term shall mean Business Associate and Covered Entity.

k. **Protected Health Information** the term “Protected Health Information” (abbreviated as “PHI”) shall mean any individually identifiable “health information” provided and/or made available by Covered Entity to Business Associate, and has the same meaning as the term “Health Information” as defined by 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. Protected Health Information includes health information in electronic form.

l. **Required By Law** shall have the same meaning as the term “required by law” in 45 CFR 164.103.

m. **Secretary** shall mean the Secretary of the Department of Health and Human Services (“HHS”) and any other officer or employee of HHS to whom the authority involved has been delegated.

n. **Security Incident** shall have the same meaning as the term “security incident” in 45 CFR 164.304.

o. **Security Rule** means the Security Standards and Implementation Specifications at

45 CFR 164.306, 164.308, 164.310, 164.312, and 164.316.

2. **Use and Disclosure of PHI**. Business Associate shall not use or further disclose PHI other than as permitted or required by this Agreement and by the HITECH Act, or as Required By Law. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of Covered Entity, provided that such use or disclosure of PHI would not violate Applicable Privacy Law if done by Covered Entity. The Business Associate is authorized to use Protected Health Information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). Except as otherwise limited in this Agreement or any other agreement between Covered Entity and Business Associate, Business Associate may also:

a. Use PHI for the proper management and administration of Business Associate contracted services or to carry out the legal responsibilities of Business Associate; and

b. Disclose PHI for the proper management and administration of 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 the information will remain confidential and be used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and that the person will notify Business Associate of any instances of which it is aware in which the confidentiality of the information may have been breached in which a Security Incident occurred.

3. **Permitted Uses and Disclosures by Business Associate.** In case Business Associate obtains or creates Protected Health Information, Business Associate may use or disclose Protected Health Information only if such use to disclosure, respectively, is in compliance with each applicable requirement of § 164.504(e) Title 45, Code of Federal Regulations. It means that:

a. **Refer to Underlying Services Agreemen**t. Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the signed agreement between the parties, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

b. **Use of Protected Health Information for Management, Administration and Legal Responsibilities.** Business Associate is permitted to use Protected Health Information if necessary for the proper management and administration of Business Associate or to carry out legal responsibilities of Business Associate.

c. **Disclosure of Protected Health Information for Management, Administration and Legal Responsibilities.** Business Associate is permitted to disclose Protected Health Information received from Covered Entity for the proper management and administration of Business Associate or to carry out legal responsibilities of Business Associate, provided:

i. The disclosure is Required By Law; or

ii. The Business Associate obtains reasonable assurances from the person to whom the Protected Health Information, including Electronic Health Information and/or Electronic Protected Health Information, is disclosed that it will be held confidentially and used or further disclosed only as Required By Law or for the purposes for which it was disclosed to the person, the person will use appropriate safeguards to prevent use or disclosure of the Protected Health Information, and the person immediately notifies the Business Associate of any instance of which it is aware in which the confidentiality of the Protected Health Information has been breached.

iii. Business Associate may use or disclose Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

d. **Data Aggregation Services.** Business Associate is also permitted to use or disclose Protected Health Information to provide data aggregation services, as that term is defined by 45 CFR 164.501, relating to the health care operations of Covered Entity.

4. **Safeguards**. Business Associate agrees to implement, maintain and use administrative, technical and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Health Information and Electronic Health Information that it creates,

receives, maintains, or transmits on behalf of the Covered Entity as required by the Privacy Rule, Security Rule, and HITECH Act 45 CFR 164.304.

5. **Mitigation.** Business Associate shall 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 Business Associate Agreement.

6. **Security Rule**. Business Associate, shall comply with applicable provisions of the Security Rule (45 CFR 164.308, 310, 312, 316 and any amendments thereto) as required by the HITECH Act, including developing and implementing written information security policies and procedures and otherwise meeting the Security Rule documentation requirements.

7. **Downstream Contracts**. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agrees in writing to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

8. **Access to PHI**. Business Associate, including its agents and subcontractors, shall provide access, at the request of Covered Entity, as soon as administratively practical and in no event later than 30 days following the Covered Entity’s request, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet Covered Entity’s requirements under 45 CFR 164.524. To the extent it maintains a Designated Record Set, 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 or an individual, as soon as administratively practicable. Business associate agrees to make Protected Health Information available for purposes of accounting of disclosure, as necessary to satisfy the Covered Entity’s obligations under 45 CFR 164.528.

9. **Amendments to PHI**. If any Individual requests an amendment of PHI directly from Business Associate or its agents or subcontractors, Business Associate must notify Covered Entity in writing. Any denial of amendment of PHI maintained by Business Associate or its agents or subcontractors shall be the responsibility of Covered Entity.

10. **Access to Books and Records**. Business Associate agrees to make internal practices, books and records relating to the use and disclosure of PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity, or at the request of Covered Entity to the Secretary, in a time and manner designated by Covered Entity or the Secretary, for purposes of determining Covered Entity’s compliance with the Privacy Rule.

11. **Documentation of Disclosures of PHI**. Within 10 days following notice by Covered Entity of subcontractors shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR 164.528. As set forth in, and as limited by, 45 CFR 164.528, Business Associate shall not provide an accounting to Covered Entity of disclosures: (a) to carry out treatment, payment or health care operations, as set forth in 45 CFR 164.502; (b) to Individuals of

PHI about them as set forth in 45 CFR 164.502; (c) to persons involved in the Individual’s care or

other notification purposes as set forth in 45 CFR 164.510; (d) for national security or intelligence purposes as set forth in 45 CFR 164.512(k)(2); or (e) to correctional institutions or law enforcement officials as set forth in 45 CFR 164.512(k)(5). Business Associate agrees to implement a process that allows for an accounting of disclosures to be collected and maintained by Business Associate and its agents or subcontractors for at least six years prior to the request, but not before the compliance date of the Privacy Rule. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual’s written authorization, or a copy of the written request for disclosure. Such requirement shall not extend to disclosures occurring prior to April 14, 2003.

12. **Confidential Communications**. Business Associate shall, if directed by Covered Entity, use alternative means or alternative locations when communicating PHI to an Individual based on the Individual’s request for confidential communications in accordance with 45 CFR 164.522.

13. **Responsibilities of the Covered Entity with Respect to Protected Health Information.**

The Covered Entity hereby agrees:

a. to advise the Business Associate, in writing, of any arrangements of the Covered Entity under the Privacy Regulations that may impact the use and/or disclosure of PHI by the Business Associate under this Agreement;

b. to provide the Business Associate with a copy of the Covered Entity’s current Notice of Privacy Practices (“Notice”) required by Section 164.520 of the Privacy Regulations and to provide revised copies of the Notice, should the Notice be amended in any way;

c. to advise the Business Associate, in writing, of any revocation of any consent or authorization of any individual and of any other change in any arrangement affecting the use and disclosure of PHI to which the Covered Entity has agreed, including, but not limited to, restrictions on use and/or disclosure of PHI pursuant to Section 164.522 of the Privacy Regulations;

d. use only if Services involve marketing or fundraising} to inform the Business Associate of any individual who elects to opt-out of any marketing and/or fundraising activities of the Covered Entity;

e. that Business Associate may make any use and/or disclosure of Protected Health Information as permitted in Section 164.512 with the prior written consent of the Covered Entity.

14. **Remuneration.** As of the effective date specified by HHS in final regulations to be issued on this topic, Business Associate shall not directly receive remuneration in exchange for any Protected Health Information of an individual unless the Covered Entity or Business Associate obtains from the individual, in accordance with 45 CFR 164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by the entity receiving Protected Health Information of that individual, except as otherwise allowed under HIPAA.

15. **Warranty for Transactions and Code Sets Rule**. If Business Associate conducts all or part of any

transaction covered by 45 CFR Part 162 with or on behalf of Covered Entity (including but not

limited to, claims payment and referral certification and authorizations), then Business Associate

covenants and warrants that it shall comply with all applicable requirements of 45 CFR 162, and

require its agents or subcontractors to comply with all applicable requirements of 45 CFR 162.

16. **Security Rule Compliance**. Business Associate shall comply with applicable provisions of the Security Rule (45 CFR 164.306, 308, 310, 312, 316 and any amendments thereto) as required by the HITECH Act, including developing and implementing written information security policies and procedures and otherwise meeting the Security Rule documentation requirements. Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with the Privacy Rule and Security Rule.

17. **Breaches and Security Incidents.**

a. Privacy or Security Breach. Business Associate will immediately report to Covered Entity any use or disclosure of Protected Health Information not permitted for by this Agreement of which it becomes aware of; and any Security Incident of which it becomes aware of. Business Associate will treat the Breach as being discovered in accordance with 45 CFR 164.410. A Breach is considered discovered on the first day the Business Associate knows or should have known about it by exercising reasonable diligence. Business Associate agrees to notify the Covered Entity of any individual whose Protected Health Information has been Breached. Business Associate agrees that such notification will meet the requirements of 45 CFR 164.410. If a delay is requested by a law- enforcement official in accordance with 45 CFR 164.412, Business Associate may delay notifying Covered Entity for the applicable time period. Business Associate’s report will at least:

i. Identify the nature of the breach or other non-permitted use or disclosure, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of any Breach, no later than 24 hours after a Breach is discovered;

ii. Identify the Protected Health Information that was subject to the non-permitted use or disclosure or Breach (such as whether full name, social security number, date of birth, home address, account number of other information were involved) on an individual basis;

iii. Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;

iv. Identify what corrective or investigational action Business Associate took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects and to protect against any further Breaches;

v. Identify what steps the individuals who were subject to a Breach should take to protect themselves;

vi. Provide such other information, including a written report, as Covered Entity may reasonably request.

b. Security Incidents. Business Associate will report to Covered Entity any attempted or successful (A) unauthorized access use, disclosure, modification, or destruction of Covered Entity’s Electronic Protected Health Information or (B) interference with Business Associate’s system operations in Business Associate’s information systems, of which Business Associate becomes aware. Business Associate will make this report monthly, except that if any such Security Incident resulted in a disclosure not permitted by this Agreement or Breach of Covered Entity’s Unsecured Protected Health Information, Business Associate will make the report in accordance with the provisions set

forth in the paragraph above.

18. **Representations and Warranties of Both Parties**

Each party represents and warrants to the other Party that:

a. it is duly organized, validly existing, and in good standing under the laws of the state in which it is organized or licensed;

b. it has the power to enter into this Agreement and to perform its duties and obligations hereunder;

c. all necessary corporate or other actions have been taken to authorize the execution of the Agreement and the performance of its duties and obligations;

d. neither the execution of this Agreement nor the performance of its duties and obligations

hereunder will violate any provision of any other agreement, license, corporate charter of bylaws of the Party;

e. it will not enter into nor perform pursuant to any agreement that would violate or interfere with this Agreement;

f. it is not currently the subject of a voluntary or involuntary petition in bankruptcy, does not currently contemplate filing any such voluntary petition, and is not aware of any claim for the filing of an involuntary petition;

g. neither the Party, nor any of its shareholders, members, directors, officers, agents, employees or contractors have been excluded or served a notice of exclusion or have been served with a notice of proposed exclusion, or have committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any Federal or state healthcare program, including but not limited to Medicare or Medicaid or have been convicted, under Federal or state law of a criminal offense;

h. all of its employees, agents, representatives and contractors whose services may use or disclose PHI on behalf of that Party have been or shall be informed of the terms of this Agreement;

i. all of its employees, agents, representatives and contractors who may use or disclose PHI on behalf of that Party are under a sufficient legal duty to the respective Party, either by contract or otherwise, to enable the Party to fully comply with all provisions of this Agreement.

Each Party further agrees to notify the other Party immediately after the Party becomes aware that any of the foregoing representation and warranties may be inaccurate or may become incorrect.

19. **Term and Termination.**

a. Term. The Term of this BA Contract shall be effective as of Effective Date, and shall terminate on the sooner of (i) the date of termination pursuant to paragraph 21b, or (ii) 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 termination provisions in the following paragraphs.

b. Termination of Agreement by Covered Entity. Upon the Covered Entity’s knowledge of a material breach of this Agreement by Business Associate, the Covered Entity shall either:

i. Provide an opportunity for the Business Associate to cure the breach and then terminate this Agreement if Business Associate does not cure the breach within the time specified by Covered Entity;

ii. Immediately terminate the Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

iii. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

c. Termination of Agreement by Business Associate. Upon the Business Associate’s knowledge of a material breach of this Agreement by Covered Entity, the Business Associate shall either:

i. Provide an opportunity for the Covered Entity to cure the breach and then terminate this Agreement if Covered Entity does not cure the breach within the time specified by Business Associate;

ii. Immediately terminate the Agreement if Covered Entity has breached a material term of this Agreement and cure is not possible; or

iii. If neither termination nor cure is feasible, Business Associate shall report the violation to the Secretary.

d. Effect of Termination of Agreement for Any Reason.

i. Except as provided in paragraph ii of this Section 20(d), upon termination of this BA Contract, for any reason, Business Associate shall promptly return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to all 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.

ii. In the event that Business Associate determines that returning or destroying Protected Health Information is infeasible, Business Associate shall promptly provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon notifying Covered Entity that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this BA Contract 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.

20. **HITECH Act**. This Agreement incorporates herein by reference the applicable provisions of Title XIII of the American Recovery and Reinstatement Act of 2009 known as the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, including but not limited to, the regulatory provisions described in 74 Federal Register 56123-56131 (October 30, 2009).

21. **Miscellaneous**

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section then in effect or as amended.

b. Amendment. The Parties agree that if Applicable Privacy Law changes, this Agreement shall be deemed to incorporate such changes as necessary in order for Covered Entity to operate in compliance with the amended or modified requirements of Applicable Privacy Law.

c. Survival. The respective rights and obligations of Business Associate under paragraphs 9, 19(c) and 19(d) shall survive the termination of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with Applicable Privacy Law.

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

f. Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with this Agreement, HIPAA or the HIPAA Regulations will be adequate or satisfactory for Business Associate’s own purposes.

g. Agreement Provisions. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of the Agreement will remain in full force and effect. In addition, in the event a Party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Privacy Rule or Security Rule, such Party shall notify the other Party in writing. For a period of up to 30 days, the Parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after such 30 day period, the Agreement fails to comply with the requirements of the HIPAA Privacy Rule and Security Rule, then either Party has the right to terminate upon written notice to the other Party. This Agreement shall be construed according to the laws of the State of New York applicable to contracts formed and wholly performed within that State. The Parties further agree that should a cause of action arise under any Federal law, the suit shall be brought in the Federal District Court where the Covered Entity is located.

21. **Entire Agreement.** This Agreement consists of this document, and constitutes the entire agreement between the Parties. There are no understandings or agreements relating to this Agreement which are not fully expressed in this Agreement and no change, waiver or discharge of obligations arising under this Agreement shall be valid unless in writing and executed by the Party against whom such change, waiver or discharge is sought to be enforced.

**INTENDING TO BE LEGALLY BOUND, the parties hereto have duly executed this Amendment as of the Effective Date.**

Business Associate Covered Entity

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_