

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the “BAA”) is entered into between the Contractor and the individual or entity whose signature appears below as evidence of agreement to these the terms hereinafter referred to as “Covered Entity.” This BAA establishes the terms of the relationship between Contractor and Covered Entity.

WHEREAS, Covered Entity is seeking confirmation by Contractor for the Centers for Disease Control and Prevention (CDC) Million Hearts Challenge (CDC Challenge) and desires to send data to Contractor and which data may include certain Protected Health Information (as defined in 45 C.F.R. § 160.103) that is subject to protection under the Federal Privacy, Security, Breach Notification, and Enforcement Rules established at 45 C.F.R. Parts 160 and 164, as amended from time to time (collectively the “HIPAA Rules”), promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009, Pub. Law No. 111-5 (“ARRA”);

WHEREAS, Contractor may act in the role of a Business Associate (as defined in 45 C.F.R. § 160.103) for purposes of Covered Entity’s assessment and review by Contractor against CDC’s standards and requirements and the HIPAA Rules dictate that the Covered Entity shall enter into an agreement with a Business Associate to whom it provides PHI, and this BAA shall apply to that PHI; and

WHEREAS, the purpose of this BAA is to satisfy certain standards and requirements of the HIPAA Rules, as the same may be amended from time to time.

NOW THEREFORE, in consideration of the mutual promises below, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

I. GENERAL PROVISIONS

Section 1. **Definitions.** Unless otherwise specified in this BAA, all capitalized terms used herein and not otherwise defined shall have the meanings established by 45 C.F.R. Parts 160 and 164, as amended from time to time. “PHI” shall mean Protected Health Information, as defined in 45 C.F.R. § 160.103, limited to the information received from or on behalf of Covered Entity. “Electronic PHI” shall mean Electronic Protected Health Information, as defined in 45 C.F.R. § 160.103, limited to the information received from or on behalf of Covered Entity. The terms “use” and “disclosure” and any and all other terms with defined meanings established by 45 C.F.R. Parts 160 and 164, as amended from time to time, shall have the same meaning for the purpose of this BAA. References in this BAA to a section or subsection of 45 C.F.R. Parts 160 and 164, and/or ARRA under Title 42 of the United States Code are references to provisions of ARRA and shall be deemed a reference to that provision and its existing and future implementing regulations, when and as each is effective and compliance is required under the applicable provision.

Section 2. **Effect.** This BAA shall apply to any PHI provided by Covered Entity to Contractor for purposes of Covered Entity's assessment against the CDC Challenge's standards and requirements. Notwithstanding anything in this Agreement to the contrary, nothing in this BAA shall alter the rights and obligations of the respective parties under the HIPAA Rules.

II. RESPONSIBILITIES OF Contractor

Section 1. **Use and Disclosure of Protected Health Information.** Contractor may:

(a) use and/or disclose PHI only as permitted or required by this BAA, or as Required By Law, and in compliance with each applicable requirement of 45 C.F.R. § 164.504(e);

(b) use the PHI in its possession for its proper management and administration and to fulfill any legal responsibilities of Contractor;

(c) disclose PHI in its possession to a third party for the purpose of Contractor's proper management and administration or to fulfill any legal responsibilities of Contractor if the disclosures are Required by Law, and Contractor has received from the third party written assurances that (i) the information will be held confidentially and be used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the third party, and (ii) the third party will notify Contractor (and, in accordance with Article II, Section 3 of this BAA, Contractor shall notify Covered Entity) of any instances of which it becomes aware in which the confidentiality of the information has been breached;

Contractor shall request, use and/or disclose the minimum amount of PHI necessary with regard to its use and/or disclosure of PHI under this Section 1. Contractor shall not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity. All other uses and disclosures of PHI not authorized by this BAA are prohibited. Contractor acknowledges that it may be subject to the civil and criminal enforcement provisions set forth at 42 U.S.C. 1320d-5 and 1320d-6, as amended from time to time, for failure to comply with the use and disclosure requirements and any guidance issued by the Secretary from time to time.

Section 2. **Appropriate Safeguards.** Contractor will use appropriate administrative, technical and physical safeguards to prevent the use or disclosure of PHI, other than as provided for by this BAA or as Required by Law, in accordance with the requirements set forth in Subpart C of 45 C.F.R. Part 164, including implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity. Contractor will also keep current and document such security measures in written policies, procedures or guidelines, and make its policies and procedures, and documentation relating to such safeguards, available to the Secretary in accordance with the HIPAA Rules.

Section 3. **Reporting of Improper Use or Disclosure of PHI.** Contractor will within ten (10) business days of becoming aware of any use or disclosure of PHI not permitted or required by or this BAA, or of any Security Incident with respect to Electronic PHI of which it becomes aware, report such use, disclosure or Security Incident to Covered Entity. Contractor

agrees to mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI by Contractor in violation of the requirements of this BAA. Contractor further agrees to report without unreasonable delay, and in no case later than thirty (30) calendar days after discovery, any Breach of any Unsecured PHI in accordance with the security breach notification requirements set forth in 45 C.F.R. §§ 164.400, 164.402, and 164.410 and any guidance issued by the Secretary from time to time.

Section 4. **Subcontractors and Agents.** Contractor agrees that any time PHI is provided or made available to its subcontractors or agents, Contractor will enter into an agreement with the subcontractor or agent that contains the same conditions and restrictions on the use and disclosure of PHI as contained in this BAA in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, and will ensure that all of its subcontractors and agents to whom it provides Electronic PHI agree to implement reasonable and appropriate safeguards to protect such Electronic PHI.

Section 5. **Right of Access, Amendment and Accounting of Disclosures.** With respect to the PHI in Contractor's possession, Contractor agrees to the following:

(a) within fifteen (15) calendar days of receiving a written request from Covered Entity, Contractor will make available to Covered Entity information necessary for Covered Entity to make an Accounting of Disclosures of PHI about an Individual in accordance with the Privacy Regulations as set forth in 45 C.F.R. § 164.528 and, in accordance with the requirements for Accounting for Disclosures made through an Electronic Health Record in 42 U.S.C. 17935(c), and when directed by Covered Entity, Contractor shall make that accounting directly to the Individual.

(b) Contractor shall record the following information regarding each disclosure of PHI subject to an Accounting of Disclosures pursuant to 45 C.F.R. § 164.528: (1) date of disclosure; (2) name of entity or person who received the PHI and, if known, the address of such entity or person; (3) a brief description of the PHI; and (4) a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure or a copy of a written request for disclosure. For multiple such disclosures of PHI to the same person or entity for a single purpose, NC Contractor QA shall provide Covered Entity, pursuant to Article II, Section 5(a) of this BAA, (1) the information set forth in Article II, Section 5(b) of this BAA regarding the first disclosure; (2) the frequency, periodicity or number of disclosures made during the accounting period; and (3) the date of the last such disclosure during the accounting period.

(c) make available its internal practices, books, and records relating to the use and disclosure of PHI to the Secretary of the Department of Health and Human Services in accordance with the HIPAA Rules; and

(d) forward to Covered Entity within five (5) business days of receiving any requests an Individual makes of Contractor pursuant to 45 C.F.R. §§ 164.524 or 164.526, so that Covered Entity may respond to such requests. Contractor shall not respond directly to those Individual requests.

Section 6. **Exchange of PHI and Communications.** Contractor agrees to the following:

(a) Contractor shall not directly or indirectly receive remuneration in exchange for any PHI in compliance with 45 C.F.R. §§ 164.502(a)(5), 164.504(e)(2)(i), and 164.508(a);

(b) Contractor shall not make or cause to be made any communication about a product or service that is prohibited by 45 C.F.R. §§ 164.502(a)(5), 164.504(e)(2)(i), and 164.508(a);

(c) Contractor shall not make or cause to be made any written fundraising communication that is prohibited by 45 C.F.R. § 164.514(f).

Section 7. **Return or Destruction of PHI.** Within thirty (30) calendar days after termination or expiration of this BAA, Contractor agrees to either return to Covered Entity or destroy all PHI received from the Covered Entity or created or received by Contractor on behalf of the Covered Entity and which Contractor still maintains in any form, including such information in possession of Contractor's subcontractors. Contractor agrees not to retain any copies of such PHI. If return or destruction of the PHI is not feasible, Contractor agrees to extend the protections, limitations and restrictions of this BAA to Contractor's use and disclosure of PHI retained after termination and to limit any further uses or disclosures to the purposes that make return or destruction infeasible.

III. OBLIGATIONS OF COVERED ENTITY

Section 1. **Limitations on Protected Health Information.** Covered Entity agrees that it will not furnish to Contractor any PHI that is subject to any restrictions on the use and/or disclosure of PHI as provided for in 45 C.F.R. § 164.522 that will affect Contractor's use or disclosure of the PHI under this BAA; provided that, with respect to restrictions that Covered Entity is required to agree to under 45 C.F.R. § 164.522(a), Covered Entity shall provide Contractor with clear written notice of those restrictions and the PHI to which they pertain.

Section 2. **Compliance with HIPAA and ARRA.** Covered Entity in performing its obligations and exercising its rights under this Agreement shall use and disclose Protected Health Information in compliance with the HIPAA Rules and ARRA. Covered Entity agrees that it will not provide to Contractor PHI unless expressly requested by Contractor in the fulfillment of this BAA.

Section 3. **Covered Entity Requests.** Covered Entity shall not request or require Contractor to use or disclose Protected Health Information in any manner that would not be permissible under the Subpart E of 45 C.F.R. Part 164 if done by Covered Entity.

IV. TERMINATION OF AGREEMENT

Section 1. **Termination of Agreement by Covered Entity.** Upon Covered Entity's knowledge of a breach of a material term of this BAA by Contractor, Covered Entity shall provide Contractor with written notice of that breach in sufficient detail to enable Contractor to understand the specific nature of that breach and afford Contractor the opportunity to cure the

breach; provided, however, if Contractor fails to cure the breach within a reasonable time specified by Covered Entity, Covered Entity may terminate this BAA. Upon termination of this BAA under this Section, Contractor will comply with the return or destruction provisions of Article II, Section 7 above.

Section 2. **Termination of Agreement by Contractor.** Upon Contractor's knowledge of a breach of a material term of this BAA by Covered Entity, Contractor shall provide Covered Entity with written notice of that breach in sufficient detail to enable Covered Entity to understand the specific nature of that breach and afford Covered Entity the opportunity to cure the breach; provided, however, if Covered Entity fails to cure the breach within a reasonable time specified by Contractor, Contractor may terminate this BAA.

V. LIMITATION OF LIABILITY

Section 1. **Hold Harmless.** Each party agrees to hold harmless the other party to this BAA from and against any and all claims, losses, liabilities, costs and other expenses (including reasonable attorney fees and costs associated with any suits, actions, proceedings, claims, or official investigations or inquiries) incurred as a result of: (i) any misrepresentation or non-fulfillment of any undertaking on the part of the party pursuant to this BAA; and (ii) negligent or intentional acts or omissions in the party's performance under this BAA. In no event will a party be responsible for any damages, caused by the failure of the other party to perform its responsibilities. If Covered Entity is an institution of a state government or a political subdivision of such state, this Article V shall apply only to the extent permitted under applicable state law, and nothing herein shall be deemed an express or implied waiver of sovereign immunity.

Section 2. **Damages.** NO PARTY SHALL BE LIABLE TO ANOTHER PARTY HERETO FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND OR NATURE RELATING TO OR ARISING FROM THE PERFORMANCE OR BREACH OF OBLIGATIONS SET FORTH IN THIS BAA, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), OR OTHERWISE, EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

VI. MISCELLANEOUS

Section 1. **Choice of Law and Jurisdiction.** The law of the District of Columbia shall govern this BAA. The parties agree that any dispute arising under this BAA shall only be resolved in a court of competent jurisdiction in the District of Columbia. Notwithstanding the foregoing, this choice of law and venue provision shall not apply if Covered Entity is an institution of a state government or a political subdivision and afforded sovereign immunity under applicable state law.

Section 2. **Change in Law.** The parties agree to negotiate to amend this BAA (a) as necessary to comply with any amendment to any provision of HIPAA or its implementing regulations, ARRA, or to comply with any other applicable laws or regulations, or amendments thereto, and/or (b) in the event any such law or regulation or amendment thereto materially alters

either party or both parties' obligations under this BAA. The parties agree to negotiate in good faith mutually acceptable and appropriate amendment(s) to this BAA to give effect to such revised obligations. If the parties are unable to agree to mutually acceptable amendment(s) within sixty (60) calendar days of the relevant change in law or regulations, either party may terminate this BAA consistent with the terms of this BAA. Notwithstanding the preceding sentence, the parties agree that this BAA is written to encompass ARRA and its implementing regulations.

Section 3. **Third Party Beneficiaries.** Nothing in this BAA shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

Section 4. **Survival.** Article I, Article II, Article V, and Article VI of this BAA shall survive termination of this BAA and continue indefinitely solely with respect to PHI Contractor retains in accordance with Article II, Section 7. Article II, Section 7 shall survive the termination of this BAA with regard to any data that Contractor possesses.

Section 5. **Notice.** Any notice, consent, request or waiver, or other communications to be given hereunder by either party shall be given in writing and will be deemed to have been given when delivered personally or by registered mail, postage prepaid and return receipt requested or by facsimile with a confirming copy placed in the United States mail addressed as provided below or to such other address as either party may designate by written notice to the other.

Section 6. **Expiration.** This BAA will expire upon the conclusion of the 20xx Centers for Disease Control and Prevention (CDC) Million Hearts Challenge.

[INTENTIONALLY LEFT BLANK]

Copy to:
Contractor

If to Covered Entity:

Name of Individual/Entity: _____

Address: _____

City/State/Zip: _____

Fax: _____

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement effective as of the date of this BAA.

Covered Entity

Print Name of Covered Entity: _____

By: _____

Print Name: _____

Title: _____

Date: _____

Contractor

By: _____

Print Name: _____

Title: _____

Date: _____