

Health Partners HIPAA Business Associate Agreement

This HIPAA Business Associate Agreement (“Agreement”) by and between Health Partners of Philadelphia, Inc., the Covered Entity (herein referred to as “HPP/CE”) and **Head Start Program**, (herein referred to as “BA”), is effective as of **June 3, 2013**:

RECITALS

Whereas,

- A. HPP/CE wishes to disclose certain information to BA pursuant to the terms of the Agreement, some of which may constitute protected health information (“PHI”);
- B. HPP/CE and BA intend to protect the privacy and provide for the security of PHI disclosed to BA pursuant to the Agreement in compliance with HIPAA and regulations promulgated by appropriate federal agencies and with other applicable laws;
- C. The purpose of this Agreement is to satisfy certain standards and requirements of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”) and the regulations promulgated there under at 45 CFR Parts 160 and 164 (the “HIPAA Regulations”), and specifically including but not limited to those HIPAA Regulations related to business associates at 45 CFR 164.504(e), 164.308(b) and 164.314(a); the amendments to HIPAA under the Health Information Technology for Economic and Clinical Health Act; and other applicable laws, as each of these laws may be amended from time to time;
- D. This agreement governs the terms and conditions under which BA will access, use or disclose PHI belonging to HPP/CE in performing services for, or on behalf of, HPP/CE pursuant to the underlying services agreement between HPP/CE and BA.

Therefore, in consideration of mutual promises below and the exchange of information pursuant to this Agreement, HPP/CE and BA agree as follows:

1. Definitions: As used in this Agreement, terms will have the same meaning given to those terms set forth in the HIPAA Regulations.
 - a. Business Associate. “Business associate” shall have the same meaning as the term “business associate” in 45 CFR 160.103.
 - b. Covered Entity. “Covered Entity” shall have the same meaning as the term “covered entity” in 45 CFR 160.103 and shall include a health plan, or a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered under the HIPAA regulations.
 - c. Protected Health Information. “Protected Health Information” or “PHI” shall have the same meaning as the term “protected health information” in 45 CFR 164.501, limited to the information created or received by BA from or on behalf of HPP/CE.

- d. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services (DHHS) or his or her designee.
- e. Required by Law. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR 154.501.
- f. HITECH or the HITECH Act. The Health Information Technology for Economic and Clinical Health Act, part of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5), which was signed into law on February 17, 2009.

2. Obligations of Business Associate:

- a. Permitted uses and disclosures: BA may use and/or disclose PHI created and/or received by BA pursuant to this Agreement solely in accordance with the specifications set forth in this Agreement, or as Required By Law (as defined in 45 CFR 164.501).
- b. Nondisclosure: BA will not use or disclose further HPP/CE's PHI otherwise than as permitted or required by this Agreement or as Required By Law.
- c. Written assurances: The parties understand that HPP/CE will receive satisfactory written] from BA that BA will adequately safeguard all PHI that it receives or creates pursuant to this Agreement.
- d. Reporting of and Response to Unauthorized Uses and Disclosures or Security Breaches, Incidents or Intrusions. BA will promptly notify HPP/CE, but in no event later than 24 hours after any suspected or actual unauthorized use or disclosure, including but not limited to any privacy or security breach, incident or intrusion, in violation of any applicable federal or state law or regulation. BA will take prompt corrective action to cure any such deficiencies and will take all actions relating the unauthorized disclosure as required by federal and state law and regulations. This requirement is in addition to the breach notification requirements for unsecured PHI described herein.
- e. BA's Agents and Subcontractors: BA will insure that any of its agents, including subcontractors, who receive PHI, will agree to the same restrictions, conditions and safeguards that apply to BA.
- f. Access to PHI: Upon the request of HPP/CE and in the time and manner requested, BA agrees to provide access to PHI in a Designated Record Set, to HPP/CE or, as directed by Covered Entity, to an individual in order to meet the requirement under 45 CFR 164.524 and the HITECH Act at 42 USC 17935(e), as applicable.
- g. Amendment of PHI: Upon the request of HPP/CE and in the time and manner requested, BA agrees to make any amendment(s) to PHI in a Designated Record Set that the HPP/CE directs or agrees to pursuant to 45 CFR 164.526.
- h. Internal Practices: BA will make its internal practices, books and records relating to the use of PHI received from HPP/CE available to all appropriate federal agencies to determine BA's compliance with HIPAA and regulations promulgated hereunder.
- i. Insurance: BA shall carry sufficient liability insurance to cover its compliance with HIPAA and regulations promulgated hereunder.
- j. Mitigation: BA agrees to establish and provide to HPP/CE upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or in violation of the HIPAA Regulations. BA further agrees to mitigate any harmful effect that is known to BA of a use or disclosure of PHI by BA in violation of this Agreement.

- k. Accounting of Disclosures: BA agrees to provide to HPP/CE or its designated individual/entity, in the timeframe and manner requested, documentation such as disclosures of PHI and information related to such disclosures as would be required to permit HPP/CE to respond to a request for an accounting of disclosures of PHI in accordance with 45 CFR 164.528 and the HITECH Act at 42 USC 17935(c), as applicable.
- l. Destruction of PHI: BA agrees that consistent with the Secretary's guidance on the destruction of PHI, the destruction of PHI on paper, film, or other hard copy media must involve either shredding or otherwise destroying the PHI so that it cannot be read or reconstructed, and that redaction is not considered a mode of destruction. Therefore, PHI must be encrypted or destroyed. BA further agrees that in order to destroy PHI on electronic media, the PHI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved. The parties acknowledge that the Secretary's guidance may be found at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>. BA agrees to comply with any additional or amended guidance or regulations from the Secretary on the destruction of PHI.
- m. Reports to Federal/State Authorities: BA may use PHI to report violations of law to appropriate Federal and/or State authorities, consistent with 45 CFR 164.502(j)(1).
- n. Application of Civil and Criminal Penalties: BA that violates any security provision of subsection (a) or (b), the provisions of sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d-5, 1320d-6) shall apply to the business associate with respect to such violation in the same manner as such sections apply to a covered entity that violates such security provision.
- o. Security Safeguards: BA shall comply with the HIPAA security requirements at 45 CFR 164.308, 164.310, 164.312, and 164.316 in the same manner that these provisions apply to HPP/CE. BA shall establish and maintain a comprehensive written privacy and security program that includes appropriate safeguards to prevent the use or disclosure of HPP/CE's PHI otherwise than as authorized by this Agreement, including: administrative safeguards, including but not limited to developing policies and procedures and conducting a risk assessment/analysis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected health information, technical safeguards, including passwords and encryption, used to protect and control access to data; security-related policies and procedures and documentation standards, and physical safeguards appropriate to the size and complexity of the BA's operations and the nature and scope of its activities to protect electronic systems and data from threats, environmental hazards, and unauthorized access. The implemented safeguards will reasonably and appropriately protect the confidentiality, integrity and availability of the electronic protected health information that BA creates, receives, maintains, or transmits on behalf of the HPP/CE.
- p. Minimum necessary: BA may only use the minimum information necessary to achieve the purpose of a use or disclosure for on behalf of CE and in accordance with this Agreement, 45 CFR 164.502(b) and the HITECH Act at 45 USC 17935(b), as may be amended. This means that BA must restrict PHI to the extent practical to the limited data set, as set forth under 45 CFR 164.514(e), and/or as otherwise provided by the Secretary.

- q. Sale of PHI; Use of PHI for Marketing and Fundraising. BA shall comply with the requirements concerning the sale of PHI, and the use of PHI for marketing and fundraising purposes, as set forth at 42 USC 17935(d), 17396(a) and 17396(b), as may be amended or interpreted by regulations.

3. Permitted Uses and Disclosures by the BA: Except as otherwise limited in this Agreement, BA may use or disclose PHI on behalf of, or to provide services to HPP/CE, as described in the underlying service agreement with HPP, if such use or disclosure of PHI would not violate the Privacy Rule if done by HPP/CE or the minimum necessary policies and procedures of the HPP/CE.

a. Specific Use and Disclosure Provisions:

- i. Except as otherwise limited in this Agreement, BA may use PHI for the proper management and administration of the BA or to carry out the legal responsibilities of the BA.
- ii. Except as otherwise limited in this Agreement, BA may disclose PHI for the proper management and administration of the BA, provided that disclosures are Required By Law, or BA 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 BA of any instances of which it is aware in which the confidentiality of the information has been breached.
- iii. Except as otherwise limited in this Agreement, BA may use PHI to provide Data Aggregation services to HPP/CE as permitted by 42 CFR § 164.504(e)(2)(i)(B).
- iv. BA may use PHI to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

4. Obligation to report violations of PHI: The HITECH Act at HIPAA Regulations at 45 CFR 164.400 et seq. impose on entities covered by HIPAA and their business associates federal breach notification requirements when "unsecured" PHI is acquired by an unauthorized party. As defined under the HIPAA Regulations, "unsecured PHI" means not secured through the use of a technology or methodology that renders the information "unusable, unreadable, or indecipherable" to unauthorized individuals in accordance with guidance issued by the Secretary at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>, as may be amended. The breach notification requirements will apply to PHI in any form.

- a. BA must report any unlawful or unauthorized access to, or use or disclosure of PHI to HPP/CE within 24 hours of when the violation is known to the BA.
- b. BA must report any unlawful or unauthorized access to, or use or disclosure of PHI to the DHHS no later than five days after the unlawful or unauthorized

access, use or disclosure has been detected. Unauthorized" means inappropriate access, review or viewing of protected health information without a direct need as defined in the agreement.

- c. As requested by HPP/CE, BA shall report any unlawful or unauthorized access to, or use or disclosure of PHI to the HPP/CE's member (or the member's representative), HHS and/or the media within the time period established by HPP/CE, which period shall be determined in order for the parties to comply with 45 CFR 164.400 et seq.

4. Obligations of HPP/CE:

- a. HPP/CE will be responsible for using appropriate safeguards to maintain and insure the confidentiality, privacy and security of PHI transmitted to BA pursuant to this Agreement, in accordance with the standards and requirements of HIPAA and HIPAA regulations until such PHI is received by BA.
- b. HPP/CE shall notify BA of any limitation(s) in its notice of privacy practices of HPP/CE in accordance with 45 CFR § 164.520, to the extent that such limitation may affect BA's use or disclosure of PHI.
- c. HPP/CE shall notify BA of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect BA's use or disclosure of PHI.
- d. HPP/CE shall notify BA of any restriction to the use or disclosure of PHI that HPP/CE has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect BA's use or disclosure of PHI.

5. Permissible Requests by HPP/CE:

- a. HPP/CE shall not request BA to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by HPP/CE.

6. Audits, Inspection and Enforcement: HPP/CE may, upon reasonable determination that BA has breached this Agreement and upon reasonable notice, inspect the facilities, systems, books and records of BA to monitor compliance with this Agreement. Failure by HPP/CE to inspect, and/or monitor compliance, does not relieve BA of its responsibility to comply with this Agreement, nor does HPP/CE's failure to detect or failure to require remediation constitute acceptance of such practice or a waiver of HPP/CE's enforcement rights under this Agreement.

7. Term & Termination:

- a. Term: The Term of this Agreement shall be effective as of the date set forth above and shall terminate when all of the PHI provided by HPP/CE to BA, or created or received by BA on behalf of HPP/CE, is destroyed or returned to HPP/CE, or, if it is infeasible to return or destroy PHI, protections are

extended to such information, in accordance with the termination provisions in this Section.

b. Termination for Cause: Upon HPP/CE's knowledge of a material breach by BA, HPP/CE shall either:

- i. Provide an opportunity for BA to cure the breach or end the violation and terminate this Agreement if BA does not cure the breach or end the violation within the time specified by HPP/CE;
- ii. Immediately terminate this Agreement if the BA has breached a material term of this Agreement and cure is not possible; or
- iii. If neither termination nor cure is feasible, HPP/CE shall report the violation to the Secretary.

c. Effect of Termination:

- i. Except as provided in paragraph (2) below, of this section, upon termination of this Agreement, for any reason, BA shall return or destroy all PHI received from HPP/CE, or created or received by BA on behalf of HPP/CE. This provision shall apply to PHI that is in the possession of any applicable subcontractors or agents of BA. BA shall retain no copies of the PHI.
- ii. In the event that BA determines that returning or destroying the PHI is infeasible, BA shall provide to HPP/CE notification of the conditions that make return or destruction infeasible. Upon notification that return or destruction of PHI is infeasible, BA 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 BA maintains such PHI.

- 8. Indemnification: BA will indemnify, hold harmless and defend HPP/CE from any claims, losses, liability, costs and other expenses incurred as a result of any misrepresentation, breach or non-fulfillment of any Agreement requirement
- 9. Certification: To the extent that HPP/CE determines that such examination is necessary to comply with HPP/CE's legal obligations under HIPAA, HPP/CE or its authorized agents may, at HPP/CE's expense, examine BA's facilities, systems, procedures and records as may be necessary for such agents to certify the extent to which the BA's security safeguards comply with HIPAA, HIPAA regulations or this Agreement.
- 10. Amendment: The parties acknowledge that state and federal laws relating to electronic data security and privacy are evolving, and that the parties may be required to amend this Agreement to insure compliance with such changes. Upon such an event, this Agreement shall incorporate any such changes, and BA will

promptly agree to any necessary amendments or a new agreement as proposed by HPP/CE, to be consistent with such changes.

11. Litigation Assistance: BA will make itself available to assist HPP/CE by testifying as witness in the event of administrative or court proceedings based on an alleged violation of HIPAA, HIPAA regulations or other laws relating to security and privacy, except where BA is also a named party in the same proceedings.
12. Third Party Beneficiaries: Nothing in this Agreement is intended to confer any rights, remedies, obligations or liabilities upon anyone other than HPP/CE, BA and their respective successors or assigns.
13. Non-assignment: This Agreement shall not be assignable by BA, without HPP/CE's prior written consent. Notwithstanding the foregoing, this Agreement shall be binding upon and shall inure to the benefit of the parties, and any successor to the operations and business of the parties whether by operation of law or otherwise.
14. Interpretation: This Agreement will be interpreted as broadly as necessary to implement and comply with HIPAA regulations and any applicable federal and state laws. The parties agree that any ambiguity in this Agreement will be resolved to permit HPP/CE to comply with HIPAA Regulations.
15. Regulatory References: A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
16. Survival: The respective rights and obligations of the BA under this Agreement shall survive the termination of this Agreement.
17. Notices: All notices and other communications required or permitted pursuant to this Agreement, shall be in writing and addressed to each party at the address set-forth below. All notices and other communications shall be mailed via registered or certified mail, return receipt requested, postage pre-paid, or transmitted by hand-delivery.

To HPP/CE:

Health Partners, Inc.
901 Market Street. Suite 500
Philadelphia, PA 19107

To BA:

Attn: Betsy Spargo
Head Start Program
3700 Vartan Way
Harrisburg, PA 17110

18. Governing Law and Venue: This Agreement shall be governed by and interpreted in accordance with the laws of the Commonwealth of Pennsylvania.

In witness thereof, the parties hereto have duly executed this Agreement as of the effective date written above.

COVERED ENTITY:
Health Partners, Inc.

By: _____

Printed Name: William S. George

Title: President and CEO

Date: _____

BUSINESS ASSOCIATE:
Head Start Program

By: _____

Printed Name: _____

Title: _____

Date: _____