ATTACHMENT 4
COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE AGREEMENT

Health Insurance Portability and Accountability Act (HIPAA) Compliance

WHEREAS, the [*name of program and/or Department*] (Covered Entity) and the **Contractor (Business Associate)**, intend to protect the privacy and provide for the security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Public Law 111-5, and the HIPAA/HITECH regulations at 45 CFR Parts 160, 162 and 164.

WHEREAS, Business Associate may receive PHI in any format including electronic form, from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI must be handled, disclosed or used only in accordance with this Attachment 5, the Underlying Agreement, and the standards established by the HIPAA Rules.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions. The following terms used in this Attachment 5 shall have the same meaning as those terms in the HIPPA/HITECH Regulations: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions:

a. "Business Associate" shall have the same meaning as the term "business associate" at 45 CFR § 160.103.
b. "Covered Entity" shall have the same meaning as the term "covered entity" at 45 CFR § 160.103.
c. "HIPAA Rules" shall mean the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Public Law 111-5, and the regulations at 45 CFR Part 160, 162, and 164.
d. "Underlying Agreement" shall mean Contract/Purchase Order # _____.

2. Changes in Law. Business Associate agrees that it will comply with any changes in the HIPAA Rules by the compliance date established by any such changes and will provide the Covered Entity with written certification of such compliance.

3. Stated Purposes for Which Business Associate May Use or Disclose PHI. Except as otherwise limited in this Attachment 5, Business Associate shall be permitted to use or disclose PHI provided by or obtained by or obtained on behalf of Covered Entity to perform those functions, activities, or services for, or on behalf of, Covered Entity which are specified in Appendix A to this Attachment 5, provided that such use or disclosure would not violate the HIPPA Rules if done by Covered Entity. Business Associate agrees to make

uses, disclosures and requests for PHI consistent with Covered Entity's minimum policies and procedures.

4. Additional Purposes for Which Business Associate May Use or Disclose Information. Business Associate shall not use or disclose PHI provided by, or created or obtained on behalf of Covered Entity for any other purposes except as required by law. Business Associate shall not use PHI to de-identify the information in accordance with 45 CFR § 164.514(a)-(c) without the Covered Entity's express written authorization(s). Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

5. Business Associate Obligations:

a. **Limits on Use and Further Disclosure Established by Appendix and Law**. Business Associate hereby agrees that the PHI provided by, or created or **obtained** on behalf of Covered Entity shall not be further used or disclosed other than as permitted or required by this Attachment 5 or as required by law.

b. **Appropriate Safeguards**. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Attachment 5 that reasonably and appropriately protects the confidentiality, integrity, and availability of the PHI that is created, received, maintained, or transmitted on behalf of the Covered Entity as required by Subpart C of 45 CFR Part 164. Appropriate safeguards shall include but are not limited to implementing:

i. administrative safeguards required by 45 CFR § 164.308;
ii. physical safeguards as required by 45 CFR § 164.310;
iii. technical safeguards as required by 45 CFR § 164.312; and
iv. policies and procedures and document requirements as required by 45 CFR § 164.316.

c. **Training and Guidance**. Business Associate shall provide annual training to relevant contractors, Subcontractors, employees, agents and representatives on how to prevent the improper use or disclosure of PHI. Business Associate shall also comply with annual guidance on the most effective and appropriate technical safeguards issued by the Secretary of Health and Human Services.

d. **Reports of Improper Use or Disclosure or Breach**. Business Associate hereby agrees that it shall notify the Covered Entity's Project Officer and the Covered Entity's Legal Office within **two (2) days** of discovery of any use or disclosure of PHI not provided for or allowed by this Attachment 5, including breaches of unsecured PHI as required by 45 CFR § 164.410. Such notification shall be written and shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during the improper use or disclosure or Breach. Business Associate shall furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to individuals under 45 CFR § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. An improper use or

disclosure or Breach shall be treated as discovered by the Business Associate on the **first day** on which it is known to the Business Associate (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of the Business Associate) or should reasonably have been known to the Business Associate to have occurred.

Business Associate Agrees that if any of its employees, agents, contractors, Subcontractors, and representatives use or disclose PHI received from, or created or received on behalf of, Covered Entity, or any derivative de-identified information, Business Associate shall ensure that such employees, agents, contractors, Subcontractors, and business representatives shall receive training on Business Associate's procedure for compliance with the HIPAA Rules. Business Associate Agrees that if any of its employees, agents, contractors, Subcontractors, and representatives use or disclose PHI received from, or created or received on behalf of, Covered Entity, or any derivative de-identified information in a manner not provided for in this Attachment 5, Business Associate shall ensure that such employees, agents, contractors, Subcontractors, and business representatives are sanctioned or prevented from accessing any PHI Business Associate receives from, or creates or receives on behalf of Covered Entity. Use or disclosure of PHI in a manner contrary to the terms of this Attachment 5 shall constitute a material breach of the Underlying Agreement.

e. **Contractors, Subcontractors, Agents and Representatives**. In accordance with 45 CFR § 164.502(e)(1)(ii) and § 164.308(b)(2), if applicable, ensure that any contractors, Subcontractors, agents and representatives that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information. The existence of any contractors, Subcontractors, agents and representatives shall not change the obligations of Business Associate to the Covered Entity under this Attachment 5.

f. **Reports of Security Incidents**. Business Associate hereby agrees that it shall notify, in writing, the Department's Project Officer within **two (2) days** of discovery of any Security Incident at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available.

g. **Right of Access to PHI**. Business Associate hereby agrees to allow an individual who is the subject of PHI maintained in a designated record set, to have access to and copy that individual's PHI within **10 business days** of receiving a written request from the Covered Entity or an authorized individual in accordance with the HIPAA Rules. Business Associate shall provide PHI in the format requested, unless it cannot readily be produced in such format, in which case it shall be provided in standard hard copy. If any individual requests from Business Associate or its contractors, Subcontractors, agents and representatives access to PHI, Business Associate shall notify Covered Entity of same within **five (5) business days**. Business Associate shall further conform with and meet all of the requirements of 45 CFR § 164.524.

h. **Amendment and Incorporation of Amendments**. Within **five (5) business days** of receiving a request from Covered Entity or from the individual for an amendment

of PHI maintained in a designated record set, Business Associate shall make the PHI available to the Covered Entity and incorporate the amendment to enable Covered Entity to comply with 45 CFR 164.526. If any individual requests an amendment from Business Associate or its contractors, Subcontractors, agents and representatives, Business Associate shall notify Covered Entity of same within **five (5) business days**.

i. **Provide Accounting of Disclosures**. Business Associate agrees to maintain a record of all disclosures of PHI in accordance with 45 CFR § 164.528. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, the purpose of the disclosure, and shall include disclosures made on or after the date which is **six (6) years** prior to the request. Business Associate shall make such record available to the individual or the Covered Entity within **10 business days** of a request for an accounting of disclosures and in accordance with 45 CFR §164.528.

j. **Access to Books and Records**. Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by Business Associate on behalf of the Covered Entity, available to the Covered Entity and the Secretary of Health and Human Services or designee for purposes of determining compliance with the HIPAA Rules.

k. **Return or Destruction of PHI**. At termination of this Attachment 5, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Attachment 5. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Attachment 5 to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

l. **Maintenance of PHI**. Notwithstanding section 4(k) of this Appendix, Business Associate and its contractors, Subcontractors, agents and representatives shall retain all PHI throughout the term of the Underlying Agreement and shall continue to maintain the information required under section 4(h) of this Appendix for a period of six (6) years after termination of the Underlying Agreement, unless Covered Entity and Business Associate agree otherwise.

m. **Mitigation Procedures**. Business Associate agrees to establish and to provide to Covered Entity 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 Attachment 5 or the HIPAA Rules. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Appendix or the Privacy Rule.

n. **Sanction Procedures**. Business Associate agrees that it shall develop and implement a system of sanctions for any contractor, Subcontractor, employee, agent and representative who violates this Exhibit or the HIPAA Rules.

o. **Application of Civil and Criminal Penalties.** All Civil and Criminal Penalties under the HIPAA Rules shall apply to Business Associate's violation of any provision contained in the HIPAA Rules.

p. **Breach Notification**. Business Associate shall comply with the Breach notification requirements of 45 CFR 164. In the event of a Breach requiring indemnification in accordance with Section 5(u), below, Covered Entity may elect to directly comply with Breach notification requirements or require Business Associate to comply with all Breach notifications requirements of 45 CFR § 164 on behalf of Covered Entity. If Covered Entity requires Business Associate to comply with Breach notification requirements, Business Associate shall provide Covered Entity with a detailed weekly, written report, starting one week following discovery of the Breach. The report shall include, at a minimum, Business Associate's progress regarding Breach notification and mitigation of the Breach. If Covered Entity elects to directly meet the requirements of 45 CFR § 164, Business Associate shall be financially responsible to Covered Entity for all resulting costs and fees incurred by Covered Entity, including, but not limited to, labor, materials, or supplies. Covered Entity may at its sole option: 1) offset amounts otherwise due and payable to Business Associate under the Underlying Agreement; or 2) seek reimbursement of or direct payment to a third party of Covered Entity's costs and fees incurred under this paragraph. Business Associate shall make payment to Covered Entity (or a third party as applicable) within **30 days** from the date of Covered Entity's written notice to Business Associate.

q. **Grounds for Breach.** Any non-compliance by Business Associate with this Attachment 5 or the HIPAA Rules will automatically be considered to be a breach of the Underlying Agreement.

r. **Termination by Commonwealth.** Business Associate authorizes termination of this Attachment 5 or Underlying Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion that the Business Associate has violated a material term of this Attachment 5.

s. **Failure to Perform Obligations**. In the event Business Associate including its contractors, Subcontractors, agents and representatives fails, to perform its obligations under this Appendix, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Attachment 5nd applicable law.

t. **Privacy Practices**. The Covered Entity will provide and Business Associate shall immediately begin using and/or distributing to clients any applicable form, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date of this

Attachment 5, or as otherwise designated by the Program or Covered Entity. The Covered Entity retains the right to change the applicable privacy practices, documents and forms. The Business Associate shall implement changes as soon as practicable, but not later than **45** days from the date of notice of the change.

u. **Indemnification**. Business Associate shall indemnify, defend and hold harmless Covered Entity from and all claims and actions, whether in law or equity, resulting from Business Associate's Breach or other violation of the HIPAA Rules (this includes but is not limited to Breach and violations by Business Associate's contractors, Subcontractors, employees, agents and representatives). Additionally, Business Associate shall reimburse Covered Entity for any civil monetary penalties imposed on Covered Entity as a result of a Breach or violation cognizable under this Section 5(u).

6. Obligations of Covered Entity:

a. **Provision of Notice of Privacy Practices**. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with 45 CFR § 164.520 (Attachment 1 to this Business Associate Appendix), as well as changes to such notice.

b. **Permissions**. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware, if such changes affect Business Associate's permitted or required uses and disclosures.

c. **Restrictions**. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR 164.522 to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

7. Survival:

The requirements, rights and obligations created by this Attachment 5 shall survive the termination of the Underlying Agreement.

Appendix A to Attachment 5, Commonwealth Business Associate Agreement

Permitted Purposes for the Creation, Receipt, Maintenance, Transmission, Use and/or Disclosure of Protected Health Information

1. Purpose of Disclosure of PHI to Business Associate: To allow _____ to meet the requirements of the Underlying Agreement.

2. Information to be disclosed to Business Associate: _____.

3. Use shall Effectuate Purpose of Underlying Agreement: _____ may use and disclose PHI to the extent contemplated by the Underlying Agreement, and as permitted by law with Commonwealth approval.