COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE APPENDIX

Health Insurance Portability and Accountability Act (HIPAA) Compliance

WHEREAS, the Pennsylvania Department of (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 HIPAA Privacy Rule (Privacy Rule), 45 CFR Parts 160 and 164, and the HIPAA Security Rule (Security Rule), 45 CFR Parts 160, 162 and 164.

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI can be used or disclosed only in accordance with this Appendix and the standards established by HIPAA and the Privacy Rule.

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, that is in electronic form, which PHI must be handled in accordance with this Appendix and the standards established by HIPAA and the Security Rule, beginning as soon as practicable but in no event later than the effective date of the Security Rule.

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

1. **Definitions.**
   a. "Business Associate" shall have the meaning given to such term under the Privacy and Security Rules, including but not limited to, 45 CFR §160.103.
   b. "Covered Entity" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 CFR §160.103.
   c. "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
   d. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164.
   e. "Protected Health Information" or "PHI" means any information, transmitted or recorded in any form or medium; (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations at 45 CFR Parts 160, 162 and 164, including, but not limited to 45 CFR §164.501.
   f. "Security Rule" shall mean the Security Standards at 45 CFR Parts 160, 162 and 164.

Obsolete

g. Terms used, but not otherwise defined, in this Appendix shall have the same meaning as those terms in 45 CFR Parts 160, 162 and 164.

2. Stated Purposes For Which Business Associate May Use Or Disclose PHI. The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for the following stated purposes, except as otherwise limited in this Agreement:

PROGRAM MUST *Include a statement describing the stated purposes that Business Associate may use or disclose the PHI. These uses and disclosures must be within the scope of the Appendix. 45 CFR §164.504(e)(2)(i).* ***If the work statement is sufficiently specific and will suffice, the following statement may be used instead.***

Stated Purposes For Which Business Associate May Use Or Disclose PHI. Except as otherwise limited in this Agreement, Business Associate shall be permitted to use or disclose PHI provided 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 this Agreement's Appendix A (Statement of Work), 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.

3. Additional Purposes For Which Business Associate May Use Or Disclose Information. In addition to the Stated Purposes, Business Associate may use or disclose PHI provided by, or created or obtained on behalf of Covered Entity for the following additional purposes(s) (***Note that this is an optional section – must decide whether or not to include it***):

a) Use Of Information For Management, Administration And Legal Responsibilities. Business Associate is permitted to use PHI if necessary for the proper management and administration of Business Associate or to carry out legal responsibilities of the Business Associate except as otherwise limited in this Agreement.

b) Disclosure Of Information For Management, Administration And Legal Responsibilities. Business Associate is permitted to disclose PHI provided by, or created or obtained on behalf of Covered Entity for the proper management and administration of Business Associate or to carry out legal responsibilities of Business Associate, except as otherwise limited in this Agreement, provided:

i) The disclosure is required by law: or

ii) The Business Associate obtains reasonable assurances in writing from any third party to whom the 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 third party, the third party will use appropriate safeguards to prevent other use or disclosure of the information, and the third party agrees to

Obsolete

immediately notify the Business Associate of any instance of which it is aware in which the confidentiality of the information has been breached.

c) **Data Aggregation Services.** Business Associate may also be permitted to use or disclose PHI to provide data aggregation services, as that term is defined by 45 CFR §164.501, if specific authorization is received from the Covered Entity.

4. 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 Appendix or as required by law.

b) **Appropriate Safeguards.** Beginning as soon as practicable but in no event later that the effective date of the Security Rule, Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Appendix. Appropriate safeguards shall include implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that is created, received, maintained, or transmitted on behalf of the Covered Entity.

c) **Reports Of Improper Use Or Disclosure.** Business Associate hereby agrees that it shall report to [*fill in name of Agreement officer for Department*] within two (2) days of discovery any use or disclosure of PHI not provided for or allowed by this Appendix.

d) **Reports Of Security Incidents.** Beginning as soon as practicable but in no event later than the effective date of the Security Rule, Business Associate shall report to [*fill in name of Agreement officer for Department*] within two (2) days of discovery any security incident of which it becomes aware.

e) **Subcontractors And Agents.** Business Associate hereby agrees that any time PHI is provided or made available to any subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Appendix.

f) **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 ten (10) business days of receiving a written request from the Covered Entity. Business Associate shall provide PHI in the format requested, unless it cannot readily be produced in such

Obsolete

format, in which case it shall be provided in standard hard copy. If any individual requests from Business Associate or its agents or subcontractors 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.

g) **Amendment And Incorporation Of Amendments.** Within ten (10) business days of receiving a request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available 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 agents or subcontractors, Business Associate shall notify Covered Entity of same within ten (10) business days.

h) **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 or April 14, 2003, whichever is later. Business Associate shall make such record available to the individual or the Covered Entity within ten (10) business days of a request for an accounting of disclosures.

i) **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 Secretary of Health and Human Services or designee for purposes of determining compliance with the HIPAA Privacy Regulations.

j) **Return Or Destruction Of PHI.** At termination of this Agreement, 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 Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Appendix 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.

k) **Maintenance of PHI.** Notwithstanding Section 5(j) of this Appendix, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under §5(h) of this Appendix for a period of six (6) years after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

Obsolete

l) 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 Appendix or the Privacy Rule. 45 CFR §164.530(f). 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.

m) Sanction Procedures. Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Appendix or the Privacy Rule.

n) Grounds For Breach. Any non-compliance by Business Associate with this Appendix or the Privacy or Security Rules will automatically be considered to be a breach of the Agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance.

o) Termination by Commonwealth. Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion, that the Business Associate has violated a material term of this Appendix.

p) Failure to Perform Obligations. In the event Business Associate 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 Appendix and applicable law.

q) Privacy Practices. The Department will provide and Business Associate shall immediately begin using 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 designated by the Program or Department. The Department 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.

5. 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, as well as changes to such notice.

Obsolete

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.

Obsolete