APPENDIX I

COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE ADDENDUM

WHEREAS, the Pennsylvania Department of Human Services (Covered Entity) and Contractor (Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide services to or on behalf of Covered Entity, in accordance with the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164,), as amended, 42 C.F.R. §§ 431.301-431.302, 42 C.F.R. Part 2, 45 C.F.R. § 205.50, 42 U.S.C. § 602(a)(1)(A)(iv), 42 U.S.C. § 1396a(a)(7), 35 P.S. § 7607, 50 Pa.C.S. § 7111, 71 P.S. § 1690.108(c), 62 P.S. § 404, 55 Pa. Code Chapter 105, 55 Pa. Code Chapter 5100, the Pennsylvania Breach of Personal Information Notification Act, 73 P.S. § 2301 *et seq*., and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance.

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 may be used or disclosed only in accordance with this Addendum and the standards established by applicable laws and agency guidance.

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 must be handled in accordance with this Addendum and the standards established by HIPAA, the HITECH Act and related regulations, and other applicable laws and agency guidance.

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

1. **Definitions.**
   a. "Business Associate" shall have the meaning given to such term under HIPAA, the HITECH Act, applicable regulations and agency guidance.
   b. "Covered Entity" shall have the meaning given to such term under HIPAA, the HITECH Act and applicable regulations and agency guidance.
   c. "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
   d. "HITECH Act" shall mean the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).
   e. "Privacy Rule" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164, as amended, and related agency guidance.
   f. "Protected Health Information" or "PHI" shall mean 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 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, the HITECH Act and related regulations and agency guidance. PHI also includes any and all information that can be used to identify a current or former applicant or recipient of benefits or services of Covered Entity (or Covered Entity's contractors/business associates).

g. "Security Rule" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.
h. "Unsecured PHI" shall mean PHI that is not secured through the use of a technology or methodology as specified in HITECH regulations and agency guidance or as otherwise defined in the HITECH Act.

2. Stated Purposes For Which Business Associate May Use Or Disclose PHI. The Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for the purposes of providing services under its contract with Covered Entity, except as otherwise stated in this Addendum.

NO OTHER DISCLOSURES OF PHI OR OTHER INFORMATION ARE PERMITTED.

3. BUSINESS ASSOCIATE OBLIGATIONS:

a) Limits On Use And Further Disclosure. Business Associate shall not further use or disclose PHI provided by, or created or obtained on behalf of Covered Entity other than as permitted or required by this Addendum or as required by law and agency guidance.

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 Addendum. 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 and limiting use and disclosure to applicable minimum necessary requirements as set forth in applicable federal and state statutory and regulatory requirements and agency guidance.

c) Reports Of Improper Use Or Disclosure. Business Associate hereby agrees that it shall report to DHS Chief Information Security Officer at (717) 772-6469**,** within two (2) days of discovery any use or disclosure of PHI not provided for or allowed by this Agreement.

d) Reports Of Security Incidents. In addition to the breach notification requirements in section 13402 of the HITECH Act and related regulations, agency guidance and other applicable federal and state laws, Business Associate shall report to DHS Chief Information Security Officer at (717) 772-6469**,** within two (2) days of discovery any security incident of which it becomes aware. At the sole expense of Business Associate, Business Associate shall comply with all federal and state breach notification requirements, including those applicable to Business Associate and those applicable to Covered Entity. Business Associate shall indemnify the Covered Entity for costs associated with any incident involving the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under federal or state law and agency guidance.

(e) Subcontractors And Agents. At any time PHI is provided or made available to Business Associate 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 Addendum.

(f) Right Of Access To PHI. Business Associate shall 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 five (5) business days of receiving a written request from the Covered Entity. Business Associate shall provide PHI in the format requested, if it is readily producible in such form and format; or if not, in a readable hard copy form or such other form and format as agreed to by Business Associate and the individual. If the request is for information maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Business Associate must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Business Associate and the individual. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity within five (5) business days. Business associate shall further conform with all of the requirements of 45 C.F.R. §164.524 and other applicable laws, including the HITECH Act and related regulations, and agency guidance.

(g) Amendment And Incorporation Of Amendments. Within five (5) 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 C.F.R. §164.526, applicable federal and state law, including the HITECH Act and related regulations, and agency guidance. If an individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within five (5) business days.

(h) Provide Accounting Of Disclosures. Business Associate shall maintain a record of all disclosures of PHI in accordance with 45 C.F.R. §164.528 and other applicable laws and agency guidance, including the HITECH Act and related regulations. 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, and the purpose of the disclosure. Business Associate shall make such record available to the individual or the Covered Entity within five (5) business days of a request for an accounting of disclosures.

(i) Requests for Restriction. Business Associate shall comply with requests for restrictions on disclosures of PHI about an individual if the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for treatment purposes), and the PHI pertains solely to a health care item or service for which the service involved was paid in full out-of-pocket. For other requests for restriction, Business Associate shall otherwise comply with the Privacy Rules, as amended, and other applicable statutory and regulatory requirements and agency guidance.

(j) Access To Books And Records. Business Associate shall 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 applicable laws and agency guidance.

(k) Return Or Destruction Of PHI. At termination or expiration of the contract, Business Associate shall return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate may not retain any copies of the PHI after termination or expiration of its contract. If return or destruction of the PHI is not feasible, Business Associate shall extend the protections of this Addendum 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 3(k) of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the its contract and this Addendum and shall continue to maintain the information required under the various documentation requirements of its contract and this Addendum (such as those in §3(h)) for a period of six (6) years after termination or expiration of its contract, unless Covered Entity and Business Associate agree otherwise.

(m) Mitigation Procedures. Business Associate shall establish and 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 Addendum or the Privacy Rules, as amended. Business Associate

shall mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Addendum or applicable laws and agency guidance.

(n) Sanction Procedures. Business Associate shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Addendum, applicable laws or agency guidance.

(o) Grounds For Breach. Non-compliance by Business Associate with this Addendum or the Privacy or Security Rules, as amended, is a breach of the contract, for which the Commonwealth may elect to terminate Business Associate's contract.

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

(q) Failure to Perform Obligations. In the event Business Associate fails to perform its obligations under this Addendum, 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 Addendum and applicable laws and agency guidance.

(r) Privacy Practices. Covered Entity 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 Covered Entity. Covered Entity may change 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. Business Associate shall otherwise comply with all applicable laws and agency guidance pertaining to notices of privacy practices, including the requirements set forth in 45 C.F.R. § 164.520.

4. 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 applicable law and agency guidance, as well as changes to such notice. Covered Entity will post on its website any material changes to its notice of privacy practices by the effective date of the material change

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 C.F.R. §164.522 and other applicable laws and applicable agency guidance, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.