APPENDIX B
COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE AGREEMENT

WHEREAS, the Commonwealth of Pennsylvania Department of Corrections ("DOC") has taken the position that it is not a "Covered entity", as defined in the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191 ("HIPAA"); and

WHEREAS, the DOC intends to protect the privacy and security of certain Protected Health Information ("PHI") to which other entities may have access pursuant to this Business Associate Agreement; and

WHEREAS, the DOC and _____ ("Business Associate") have agreed to enter into this Business Associate Agreement to memorialize the privacy and security protections of certain PHI to which Business Associate may have access in order to provide goods or services to or on behalf of the DOC, in accordance with HIPAA, , the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the *American Recovery and Reinvestment Act of 2009* (ARRA), as amended, 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*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329, and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance; and,

WHEREAS, Business Associate may receive PHI from the DOC, or may create or obtain PHI from other parties for use on behalf of the DOC, which PHI may be used or disclosed only in accordance with this Business Associate Agreement and the standards established by applicable laws and agency guidance; and

WHEREAS, Business Associate may receive PHI from the DOC, or may create or obtain PHI from other parties for use on behalf of the DOC, which PHI must be handled in accordance with this Business Associate Agreement and the standards established by HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and other applicable laws and agency guidance.

NOW, THEREFORE, the DOC and Business Associate, intending to be legally bound, agree as follows:

1. Definitions.

(a) "**Business Associate**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(b) "**HIPAA**" shall mean the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191.

(c) "**HITECH Act**" shall mean the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, 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).

(d) "**Parties**" shall mean the DOC and the Business Associate, collectively.

(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 have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule (all as amended) and agency guidance.

(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 Act regulations, as amended, and agency guidance or as otherwise defined in the HITECH Act, as amended.

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 stated in this Business Associate Agreement:

Information may be used or shared for the following purposes: providing recommendations for treatment or services; reporting of compliance with treatment, including required parole conditions; and coordination of services to meet reentrant needs, including referrals to other DOC-covered services as well as referrals to other community resources.

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, the DOC other than as permitted or required by this Business Associate Agreement, as requested by the DOC, 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 Business Associate Agreement. 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 DOC 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 the Regional Program Manager at PA Department of Corrections, 1920 Technology Parkway, Mechanicsburg, PA 17050, within **two (2) days** of discovery any use or disclosure of PHI not provided for or allowed by this Business Associate Agreement.

(d) **Reports on Security Incidents**. In addition to following the breach notification requirements in section 13402 of the *Health Information Technology for Economic and Clinical Health Act of 2009* ("HITECH Act"), as amended, and related regulations, the Privacy Rule, the Security Rule, agency guidance and other applicable federal and state laws, Business Associate shall report to the Regional Program Manager at PA Department of Corrections, 1920 Technology Parkway, Mechanicsburg, PA 17050 **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 the DOC. Business Associate shall indemnify the DOC 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. For purposes of the security incident reporting requirement, inconsequential unsuccessful incidents that occur on a daily basis, such as scans, "pings," or other unsuccessful attempts to penetrate computer networks or servers containing electronic PHI maintained by Business Associate, need not be reported in accordance with this section, but may instead be reported in the aggregate on a monthly basis.

(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

substantially the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Business Associate Agreement.

(f) **Right of Access to PHI**. For any PHI maintained in a designated record set, Business Associate shall allow the DOC to have access to and copy an individual's PHI within **five (5) business days** of receiving a written request from the DOC. 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 DOC 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 DOC. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify the DOC 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, as amended, related regulations and agency guidance. Business Associate shall indemnify the DOC for all costs and damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(f).

(g) **Amendment and Incorporation of Amendments**. Within **five (5) business days** of receiving a written request from the DOC for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable the DOC to comply with 45 C.F.R. § 164.526, applicable federal and state law, including the HITECH Act , as amended and related regulations, the Privacy Rule, the Security Rule and agency guidance. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify the DOC within **five (5) business days**.

(h) **Provide Accounting of Disclosures**. Business Associate shall maintain a record of all disclosures of PHI made by Business Associate which are not excepted from disclosure accounting requirements under HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule (all as amended), in accordance with 45 C.F.R. § 164.528 and other applicable laws and agency guidance, including the HITECH Act, as amended, 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 DOC within **five (5) business days** of a written request for an accounting of disclosures. Business Associate shall indemnify the DOC for all costs and damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(h).

(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 Rule, 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 DOC, 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 of this Business Associate Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of the DOC. Business Associate agrees not to retain any copies of the PHI after termination of this Business Associate Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Business Associate Agreement 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 the DOC that the PHI has been destroyed.

(l) **Maintenance of PHI**. Notwithstanding subsection 3(k) of this Business Associate Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of this Business Associate Agreement and shall continue to maintain the information required under the various documentation requirements of this Business Associate Agreement (such as those in subsection 3(h)) for a period of **six (6) years** after termination of this Business Associate Agreement, unless Covered Entity and Business Associate agree otherwise.

(m) **Mitigation Procedures**. Business Associate agrees to establish and to provide to the DOC, 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 Business Associate Agreement or the Privacy Rule, as amended. 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 Business Associate Agreement or applicable laws and agency guidance.

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

(o) **Grounds for Breach**. Non-compliance by Business Associate with this Business Associate Agreement or the Privacy or Security Rules, as amended, is a breach of this Business Associate 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. The DOC may elect to terminate Business Associate's contract for such breach.

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

(q) **Failure to Perform Obligations**. In the event Business Associate fails to perform its obligations under this Business Associate Agreement, the DOC may immediately discontinue providing PHI to Business Associate. The DOC may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by the DOC and reporting by Business Associate, as the DOC, in its sole discretion, determines to be necessary to maintain compliance with this Business Associate Agreement and applicable laws and agency guidance.

(r) **Privacy Practices**. The DOC will provide Business Associate with all applicable forms, 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 the DOC. The DOC may change applicable privacy practices, documents and forms. The Business Associate shall make reasonable endeavors to 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 THE DOC.

(a) **Permissions**. The DOC shall provide Business Associate with any changes in, or revocation of, permission by an individual to use or disclose PHI of which the DOC is aware, if such changes affect Business Associate's permitted or required uses and disclosures.

(b) **Restrictions**. The DOC shall notify Business Associate in writing of any restriction to the use or disclosure of PHI that the DOC has agreed to in accordance with 45 C.F.R. § 164.522, as amended, and other applicable laws and applicable agency guidance, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(c) **Requests**. The DOC shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA, HITECH and related

regulations, the Privacy Rule or the Security Rule, all as amended, if done by the DOC.

5. MISCELLANEOUS.

(a) **Regulatory References**. A reference in this Business Associate Agreement to a section in HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule refers to the most current version of the section in effect or as amended.

(b) **Amendment**. The Parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time in order to ensure compliance with the requirements of the HIPAA, HITECH and related regulations, the Privacy Rule, the Security Rule and any other applicable law, all as amended.

(c) **Conflicts**. In the event that any terms of this Business Associate Agreement are inconsistent with the terms of the Agreement entered into by the DOC and Business Associate, then the terms of this Business Associate Agreement shall control.

The parties, through their authorized representative, have signed this Agreement below.

BUSINESS ASSOCIATE	**COMMONWEALTH OF PENNSYLVANIA DEPARTMENT OF CORRECTIONS**
_____	_____
Signature	Signature
_____	_____
Name Date	Name Date
_____	_____
Title	Title

SAP Vendor No. _____