

**EXHIBIT F**  
**HEALTH CARE PLAN CONSULTING AND MANAGEMENT SERVICES**  
**AGREEMENT FOR HEALTH OPTIONS PROGRAM**  
**(INCLUDING MEDICARE PRESCRIPTION DRUG PLAN)**

**HIPAA BUSINESS ASSOCIATE AGREEMENT**

[THIS HIPAA BUSINESS ASSOCIATE AGREEMENT ("**BAA**") is made and entered into as of this \_\_\_\_ day of \_\_\_\_\_, \_\_\_\_ ("**Effective Date**") by and between [PLACEHOLDER FOR VENDOR NAME ] [PLACEHOLDER FOR LEGAL ENTITY TYPE AND JURISDICTION OF FORMATION] ("**Business Associate**"), whose principal place of business is [PLACEHOLDER FOR PRINCIPAL PLACE OF BUSINESS] and the Commonwealth of Pennsylvania, Public School Employees' Retirement Board ("**Board**"), for and on behalf of the health plan sponsored by the Board and known as the [PLACEHOLDER FOR NAME OF THE COVERED ENTITY ("referred to herein as the "**Covered Entity**")], whose principal place of business is 5 North 5th Street, Harrisburg, Pennsylvania 17101.

[PLACEHOLDER FOR ALTERNATIVE INTRODUCTORY PARAGRAPH]

**RECITALS:**

**WHEREAS**, as provided in the Act of May 17, 2001 (P.L. 26, No. 9), the General Assembly of the Commonwealth of Pennsylvania enacted the Public School Retirees' Health Insurance Act, Title 24, Pa. C.S. §§ 8701 - 9102 ("**Health Act**") to provide for the sponsorship of a group health insurance program to make available health care benefits to each eligible person as defined in the Health Act;

**WHEREAS**, in furtherance of the directive of the Health Act, the Board sponsors the Covered Entity;

**WHEREAS**, the Health Act gives the Board administrative powers to administer the Covered Entity, including, but not limited to, to contract for services, consultants and other professional personnel as needed to operate the Covered Entity;

**WHEREAS**, concurrently with this BAA, the Board and the Business Associate have entered into an agreement under which the Business Associate has agreed to provide services to the Covered Entity ("**Agreement**");

**WHEREAS**, in providing services to the Covered Entity, the Business Associate may receive from the Covered Entity, or may create, or obtain from other parties, for use on behalf of the Covered Entity, Protected Health Information (as defined below);

**WHEREAS**, the Board, for and on behalf of the Covered Entity, and the Business Associate are committed to complying with all federal and state laws governing the confidentiality

and privacy of “protected health information”, as defined in 45 C.F.R. §§ 164.501 and 160.103, including but not limited to, the Health Insurance Portability and Accountability Act of 1996, as amended, Pub. L. No. 104-191 (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 their related regulations, the HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164, as amended, and the HIPAA Security Rule, 45 C.F.R. Parts 160, 162 and 164), as amended; and

**WHEREAS**, the Board, for and on behalf of the Covered Entity, and the Business Associate intend to protect the privacy and provide for the security of Protected Health Information the Business Associate may receive from the Covered Entity, or may create, or obtain from other parties, for use on behalf of the Covered Entity.

**NOW, THEREFORE**, effective as of the Effective Date, in consideration of the foregoing recitals, which are incorporated herein, and the mutual promises and undertakings hereinafter set forth, the exchange of information pursuant to the Agreement and this BAA, and intending to be legally bound hereby, the Board, on behalf of the Covered Entity, and the Business Associate, agree as follows:

## **1. Definitions.**

For purposes of this BAA, the following terms shall be defined as follows:

- (a) **“Breach”** means the acquisition, access, use, or disclosure of “protected health information”, as defined in 45 C.F.R. §§ 164.501 and 160.103 in a manner not permitted under the Privacy Rule which compromises the security or privacy of the “protected health information,” as this term “Breach” is defined in 45 C.F.R. §164.402.
- (b) **“Business Associate”** has the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance. The Board and the Business Associate agree that the Business Associate constitutes a “Business Associate” within the meaning of this definition.
- (c) **“Covered Entity”** has the meaning given to such the term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance. The Board and the Business Associate agree that the Health Options Program constitutes a “Covered Entity” within the meaning of this definition.
- (d) **“Designated Record Set”** has the meaning given to such term under the Privacy Rule, including 45 C.F.R. § 164.501.

- (e) “**HIPAA**” means the Health Insurance Portability and Accountability Act of 1996, as amended, Pub. L. No. 104-191.
- (f) “**HIPAA Rules**” means all federal laws governing the confidentiality and privacy of “protected health information”, as defined in 45 C.F.R. §§ 164.501 and 160.103, including but not limited to, HIPAA, HITECH and their related regulations, the Privacy Rule and the Security Rule.
- (g) “**HITECH Act**” means 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).
- (h) “**Privacy Rule**” means the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and Part 164.
- (i) "**Protected Health Information**" or "**PHI**" has 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, limited to the “protected health information”, as defined in such laws, regulations and guidance, created or received by the Business Associate from or on behalf of the Covered Entity.
- (j) “**Required by Law**” means a mandate contained in law that compels an entity to make a use or disclosure of “protected health information” as defined in 45 C.F.R. §§ 164.501 and 160.103 and that is enforceable in a court of law. Required by Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits, as defined in 45 C.F.R. § 164.402.
- (k) “**Security Incident**” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as defined in 45 C.F.R. § 164.304.
- (l) "**Security Rule**" means the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.
- (m) “**Services**” means the functions, activities, or services for, or on behalf of, the Covered Entity which the Business Associate has agreed to perform under the Agreement.

- (n) **“Unsecured PHI”** means any “protected health information”, as defined in 45 C.F.R. §§ 164.501 and 160.103 that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in the guidance issued under Section 13402(h)(2) of Public Law 111-5.
2. **Permitted Uses of PHI.** The Business Associate may use PHI only as permitted or required by this BAA for the following purposes: (a) as necessary to provide the Services; (b) to carry out its legal responsibilities; (c) for the proper business management and administration of the Business Associate; and (d) as Required by Law.
3. **Permitted Disclosures of PHI.** The Business Associate may disclose PHI only as permitted or required by this BAA for the following purposes: (a) as necessary to provide the Services; (b) for the proper business management and administration of the Business Associate or to carry out its legal responsibilities, provided that the Business Associate has obtained written reasonable assurances that the recipient will (i) hold such PHI in confidence, (ii) use or further disclose the PHI only for the purpose for which the PHI was received or as Required by Law, and (iii) notify the Business Associate of any instance of which the recipient becomes aware in which the confidentiality of such PHI has been breached; and (c) for the proper business management and administration of the Business Associate or to carry out its legal responsibilities, if Required by Law; provided, however, that any disclosure to an agent or subcontractor of the Business Associate shall be pursuant to a written agreement between the Business Associate and such agent or subcontractor containing substantially the same restrictions and conditions on the use and disclosure of PHI as are set forth in this BAA.
4. **Prohibited Uses and Disclosures.** The Business Associate shall not further use or disclose PHI (a) other than as permitted or required by this BAA or as Required by Law and (b) in a manner that would violate the HIPAA Rules if done by the Covered Entity. The Business Associate shall not sell PHI or use or disclose PHI for purposes of marketing or fundraising. Unless the Covered Entity gives its prior, express written consent, the Business Associate shall not de-identify any PHI except as necessary to provide the Services and unless expressly provided otherwise in a written agreement between the Board and the Business Associate. As between the Business Associate and the Covered Entity, all de-identified PHI shall be and remain exclusively the property of the Covered Entity, (a) the Business Associate assigns to the Covered Entity all of the Business Associate's right, title, and interest therein, if any, and (b) the Business Associate shall not use any such de-identified PHI for any purpose other than to provide the Services and shall not disclose the same to any third party except with the prior written consent of the Covered Entity or as otherwise required by applicable law or upon the order of a court of competent jurisdiction.
5. **Business Associate Obligations.**
- (a) **Appropriate Safeguards.** The Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided in this BAA 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 Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 164. Appropriate safeguards shall include, but are not limited to implementing:

- (i) administrative safeguards required by 45 C.F.R. § 164.308;
  - (ii) physical safeguards as required by 45 C.F.R. § 164.310;
  - (iii) technical safeguards as required by 45 C.F.R. § 164.312; and
  - (iv) policies and procedures and document requirements as required by 45 C.F.R. § 164.316.
- (b) **Training and Guidance.** The 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. The 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.
- (c) **Reports of Improper Use or Disclosure or Breach.** The Business Associate hereby agrees that it shall notify the Director of the PSERS Health Insurance Office 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 BAA, including Breaches of Unsecured PHI as required by 45 C.F.R. § 164.410. Such notification shall be written and shall include the identification of each individual whose PHI constitutes 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. The Business Associate shall furnish the Covered Entity with any other available information that the Covered Entity is required to include in its notification to individuals under 45 C.F.R. § 164.404(c) at the time of the Business Associate's notification to the 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, contractor, subcontractor, representative or other agent of the Business Associate) or should reasonably have been known to the Business Associate to have occurred.
- (d) **Training.** The Business Associate agrees that if any of its employees, contractors, subcontractors, agents or representatives use or disclose PHI received from, or created or received on behalf of, the Covered Entity, or any derivative de-identified information, the Business Associate shall ensure that such employees, contractors, subcontractors, agents and representatives shall receive training on the Business Associate's procedure for compliance with the HIPAA Rules. The Business

Associate agrees that if any of its employees, contractors, subcontractors, agents or representatives use or disclose PHI received from, or created or received on behalf of, the Covered Entity, or any derivative de-identified information in a manner not provided for in this BAA, the Business Associate shall ensure that such employees, contractors, subcontractors, agents and representatives are sanctioned or prevented from accessing any PHI that the Business Associate receives from, or creates or receives on behalf of the Covered Entity. Use or disclosure of PHI in a manner contrary to the terms of this BAA shall constitute a material breach of the Agreement.

- (e) **Contractors, Subcontractors, Agents and Representatives.** In accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 164.308(b)(2), if applicable, the Business Associate shall 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 the Business Associate to the Covered Entity under this BAA.
- (f) **Reports of Security Incidents.** The Business Associate hereby agrees that the Business Associate shall notify, in writing, the Director of the PSERS Health Insurance Office within **two (2) days** of discovery of any Security Incident at the time of Business Associate's notification to the Covered Entity or promptly thereafter as such information becomes available.
- (g) **Right of Access to PHI.** The 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. The 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 the Business Associate or its contractors, subcontractors, agents or representatives, access to PHI, the Business Associate shall notify the Covered Entity of same within **five (5) business days**. The Business Associate shall further conform with and meet all of the requirements of 45 C.F.R. § 164.524.
- (h) **Amendment and Incorporation of Amendments.** Within **five (5) business days** of receiving a request from the Covered Entity or from the individual for an amendment of PHI maintained in a Designated Record Set, the Business Associate shall make the PHI available to the Covered Entity and incorporate the amendment to enable the Covered Entity to comply with 45 C.F.R. § 164.526. If any individual requests an amendment from the Business Associate or its contractors, subcontractors, agents or representatives, the Business Associate shall notify the Covered Entity of same within **five (5) business days**.

- (i) **Provide Accounting of Disclosures.** The Business Associate agrees to maintain a record of all disclosures of PHI in accordance with 45 C.F.R. § 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. The 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 C.F.R. § 164.528.
- (j) **Access to Books and Records.** The Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, created or received by the 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 BAA, the Business Associate hereby agrees to return or destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity. The Business Associate agrees not to retain any copies of the PHI after termination of this BAA. If return or destruction of the PHI is not feasible, the Business Associate agrees to extend the protections of this BAA to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If the Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.
- (l) **Maintenance of PHI.** Notwithstanding subsection 5(k) of this BAA, the Business Associate and its contractors, subcontractors, agents and representatives shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under subsection 5(i) of this BAA for a period of **six (6) years** after termination of the Agreement, unless the Covered Entity and Business Associate agree otherwise.
- (m) **Mitigation Procedures.** The Business Associate agrees to establish and to provide to the 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 BAA or the HIPAA Rules. The Business Associate further agrees to mitigate any harmful effect that is known to the Business Associate of a use or disclosure of PHI by the Business Associate in violation of this BAA or the Privacy Rule.
- (n) **Sanction Procedures.** The Business Associate agrees that the Business Associate shall develop and implement a system of sanctions for any contractor, subcontractor, employee, agent and representative who violates this BAA or the HIPAA Rules.

- (o) **Application of Civil and Criminal Penalties.** All civil and criminal penalties under the HIPAA Rules shall apply to the Business Associate's violation of any provision contained in the HIPAA Rules.
- (p) **Breach Notification.** The Business Associate shall comply with the breach notification requirements of 45 C.F.R. Part 164. In the event of a Breach requiring indemnification and hold harmless in accordance with subsection 5(u), below, the Covered Entity may elect to directly comply with breach notification requirements or require Business Associate to comply with all breach notifications requirements of 45 C.F.R. Part 164 on behalf of the Covered Entity. If the Covered Entity requires the Business Associate to comply with breach notification requirements, the Business Associate shall provide the Covered Entity with a detailed weekly, written report, starting one week following discovery of the Breach. The report shall include, at a minimum, the Business Associate's progress regarding breach notification and mitigation of the Breach. If the Covered Entity elects to directly meet the requirements of 45 C.F.R. Part 164, the Business Associate shall be financially responsible to the Covered Entity for all resulting costs and fees incurred by the Covered Entity, including, but not limited to, labor, materials, or supplies. The Covered Entity may at its sole option:
  - (i) Offset amounts otherwise due and payable to Business Associate under the Agreement; or
  - (ii) Seek reimbursement of or direct payment to a third party of the Covered Entity's costs and fees incurred under this subsection.

The Business Associate shall make payment to the Covered Entity (or a third party as applicable) within **30 days** from the date of the Covered Entity's written notice to the Business Associate.

- (q) **Grounds for Breach.** Any non-compliance by the Business Associate with this BAA or the HIPAA Rules will automatically be considered to be a breach of the Agreement.
- (r) **Termination by Board.** The Business Associate authorizes termination of this BAA or the Agreement by the Board if the Board determines, in its sole discretion that the Business Associate has violated a material term of this BAA.
- (s) **Failure to Perform Obligations.** In the event the Business Associate including its contractors, subcontractors, agents and representatives fails, to perform its obligations under this BAA, the Covered Entity may immediately discontinue providing PHI to the Business Associate. The Covered Entity may also, at its option, require the Business Associate to submit to a plan of compliance, including monitoring by the Covered Entity and reporting by the Business Associate, as the



Covered Entity in its sole discretion determines to be necessary to maintain compliance with this BAA and 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 BAA, or as otherwise designated by the 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.** The Business Associate shall indemnify and hold harmless the Board, its members and their designees, the Covered Entity, and each of the directors, officers, agents and employees of the foregoing, and each employee of the Commonwealth of Pennsylvania, Public School Employees' Retirement System (a/k/a/ PSERS) (each of the foregoing individually and collectively an "**Indemnified Party**") from and against any and all damages, claims, demands, suits, costs, disbursements, actions, expenses, liabilities, losses, settlements, judgments, civil monetary penalties, of any nature, including attorney's fees and disbursements (individually and collectively "**Claim**") suffered or incurred by the Indemnified Party which arise out of or result from any breach or violation of any covenant, obligation or duty under this BAA or violation of the HIPAA Rules by the Business Associate or any officer, employee, contractor, subcontractor, agent or representative of the Business Associate. Pursuant to the Commonwealth Attorneys Act (71 P.S. Section 732-101, et seq.), the Office of Attorney General ("**OAG**") has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under such terms as it deems appropriate, delegate its right of defense. If delegated, the Business Associate shall defend at the Business Associate's expense, actions brought against each Indemnified Party, based upon any such Claim and the cost of such defense shall be borne by the Business Associate. Further, the Board, on behalf of the Covered Entity, agrees to cooperate with all reasonable requests of the Business Associate made in the defense of such suits. Neither the Board nor the Business Associate may enter into a settlement of any claim or suit without the other party's written consent, which will not be unreasonably withheld.
- (v) **Minimum Necessary.** The Business Associate shall request, use, and disclose only the minimum necessary amount of PHI to provide the Services.
- (w) **Assistance in Litigation or Administrative Proceedings.** The Business Associate shall make itself, and any subcontractors, employees or agents assisting the Business Associate in the performance of its obligations under the Agreement or this BAA, available to the Board and the Covered Party, at no cost to the Board or the Covered Party, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Board or the Covered

Party, its directors, officers, or employees, based upon claimed violation of the HIPAA Rules or other laws relating to security and privacy, except where the Business Associate or its subcontractor, employee, agent or representative is a named adverse party.

**6. Obligations of Covered Entity.**

- (a) **Provision of Notice of Privacy Practices.** The Covered Entity shall provide the Business Associate with the notice of privacy practices that the Covered Entity produces pursuant to the HIPAA Rules as well as changes to such notice.
- (b) **Permissions.** The Covered Entity shall provide the Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which the Covered Entity is aware, if such changes affect the Business Associate's permitted or required uses and disclosures.
- (c) **Restrictions.** The Covered Entity shall notify the 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 to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

**7. Changes in Law.** The Business Associate agrees that the Business Associate shall 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.

**8. Interpretation.** This BAA shall be interpreted as broadly as necessary to implement and comply with the HIPPA Rules.

**9. Survival.** The requirements, rights and obligations created by this BAA shall survive the termination or expiration of the Agreement.

[PLACEHOLDER FOR COUNTERPARTS, OTHER MISCELLANEOUS PROVISIONS, CLOSING PARAGRAPH AND SIGNATURE BLOCKS IF BAA IS SEPARATELY EXECUTED]