™

PUBLIC EDUCATION EMPLOYEES' HEALTH INSURANCE PLAN

Business Associate Policy

December 8, 2015

The Public Education Employees' Health Insurance Plan ("PEEHIP") protects the privacy of personal information in accordance with applicable privacy laws. PEEHIP is required by law to take reasonable steps to ensure the privacy of our members' healthcare information in accordance with the Health Insurance Portability and Accountability Act (**HIPAA**). With the addition of the Health Information Technology for Economic and Clinical Health (**HITECH**) Act, (enacted as part of the American Recovery and Reinvestment Act of 2009), and the final set of rules included in the HIPAA Omnibus rule set in 2013, it is imperative that PEEHIP maintain reasonable oversight over protected health information that it shares with its business associates. As defined by HIPAA, a "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

Policy:

PEEHIP shall ensure that all of its business associate agreements (BAA's) meet current regulation requirements and are reviewed annually by internal staff or others. Any addendum(s) to a BAA that are required by any current or proposed HIPAA or HITECH statutes or regulations shall be entered into within the time frame mandated pursuant to such statutes or regulations.

As a continued or future business associate of PEEHIP, business associates must provide adequate documentation stating they are in compliance with current HIPAA Security and Privacy rules. Documentation must consist of, at a minimum, one of the following:

- **External HIPAA Attestation Report**

  A HIPAA attestation report must be conducted by a credible third party audit firm specializing in HIPAA Privacy and Security audits within the last year. Assessments must continue to be scheduled on a regular yearly basis covering at minimum the last 12 consecutive months of the previous year and not a point in time. The assessment must provide a qualified opinion of whether the business associate meets current HIPAA and HITECH Security and Privacy requirements based on an agreed-upon set of procedures (AUP). Report must be signed by a certified CISA, CISSP, or HCISPP auditor.

- **Service Organization Control Reporting**

  Service Organization Control reports are required by business associates based upon service(s) performed on behalf of PEEHIP. Business associates classified as having a material impact on PEEHIP's financial statement will be required to obtain a **SOC 1 Type 2** report as deemed necessary by PEEHIP. Organizations which provide services to PEEHIP with direct access to public health information (PHI) will be required to complete a **SOC 2 Type 2** relevant to the service(s) being performed by the business associate. A **SOC 2 Type 2** report is required for each trust service principle that is relevant to the outsourced service being performed by the business associate. In most cases PEEHIP will require each business associate to audit their controls against all five trust services principles including: **security**, **privacy**, **availability**, **confidentiality**,

and **processing integrity**. The SOC 2 Type 2 report must be performed directly on the business associate covering the last 12 consecutive months.

If the business associate utilizes or will utilize a managed data service provider or "subservice" such as Amazon or Microsoft Azure Cloud Services, the business associate will be required to produce a separate **SOC 2 Type 2** report based upon contracted service type(s). This report must also cover the last 12 consecutive months without gap.

- Note: For "subservice" providers, a **SOC 2 Type 2** report must include at minimum the following trust services principles: **security**, **availability**, and **confidentiality**. If the "subservice" provider also performs data processing functions for the business associate, the remaining trust service principles, **processing integrity** and **privacy,** will be required as part of the **SOC 2 Type 2** report.

- **HITRUST Certification**
  The HITRUST Common Security Framework (CSF) is a comprehensive and certifiable security framework used by healthcare organizations and their business associates to efficiently approach regulatory compliance and risk management. A current HITRUST certification issued within the last year will be accepted by PEEHIP to meet compliance with this policy.

Policy Enforcement:

If any current or future business associate plans to obtain one of the reports or certifications noted above but currently does not possess it, PEEHIP will accept the following:

- For current business associates, a proof of engagement letter stating they will complete and provide one of the acceptable reports or certifications to PEEHIP within 12 months.
- For new business associates, a proof of engagement letter stating they will complete and provide one of the acceptable reports or certifications to PEEHIP within 90 days of executing the contract.

Initial reports must incorporate more than 90 days' worth of data for testing, while subsequent reports must include the last 12 months of controls testing without gap. If a current business associate fails to comply with this Policy, PEEHIP shall have the right, at PEEHIP's sole discretion, to request one of the above defined audits to be completed and results obtained within a period of time defined by PEEHIP from the date such business associate receives written notice of noncompliance from PEEHIP**. In such event, the audited party will be solely responsible for all expenses incurred by the parties during the audit, including without limitation, all payment due to the audit firm. Should such business associate not agree to an audit within 90 days of receiving written notice of noncompliance from PEEHIP, PEEHIP shall have the right, in its sole discretion, to terminate its relationship with the business associate and/or to impose any such other penalties as PEEHIP may have the right to impose pursuant to the applicable contract and governing law.**

BIDDER/PROPOSER VERIFICATION OF ADHERENCE TO THE

PEEHIP BUSINESS ASSOCIATE POLICY

1. On behalf of the Bidder or Proposer for this solicitation, I confirm that I have read the PEEHIP Business Associate Policy dated December 8, 2015.

2. Bidder/Proposer is in compliance with current HIPAA Security and Privacy rules, as contemplated under the PEEHIP Business Associate Policy as of the date of this Verification.

3. Bidder/Proposer shall timely submit the following documentation of such compliance (please check all that apply):

_____ a. External HIPAA Attestation Report

_____ b. Service Organization Control Report

_____ c. HITRUST Certification

_____ d. Proof of Engagement Letter stating Bidder/Proposer will complete and provide one of the acceptable reports or certifications to PEEHIP within 180 days of a signed contract with PEEHIP.

4. I have full authority to represent and bind Bidder/Proposer.

Name of Bidder or Proposer: _____

Dated: _____

Signature: _____

Print Name: _____

Title: _____