

REQUEST FOR PROPOSALS

FOR

**ACTUARIAL SERVICES RELATING TO HEALTH CARE COSTS
AND BENEFITS INCLUDING SERVICES FOR THE VALUATION
OF OTHER POST-EMPLOYMENT BENEFITS (OPEB)**

FOR

THE

**ALABAMA RETIRED EDUCATION EMPLOYEES'
HEALTH CARE TRUST**

AND

**PUBLIC EDUCATION EMPLOYEES' HEALTH
INSURANCE PLAN**

PERFORMED FOR THE

FISCAL YEARS 2015-2019

RFP 1600000006

THIS RFP CONTAINS INFORMATION UNDER THE FOLLOWING HEADINGS:

SECTION I—General Information for the Proposer

- A. Purpose
- B. Background
- C. Description of the Trust's Management
- D. Other Information
- E. Proposal Opening
- F. Delivery Schedule
- G. Payment Schedule
- H. Selection of Firm
- I. Economy of Preparation
- J. News Releases
- K. Addenda to the RFP
- L. Contact Point
- M. Minimum Qualifications
- N. State of Alabama Contract Requirements

SECTION II—Nature of Services Required

- A. Purpose
- B. Required Services

SECTION III-- Information Required from Proposers

SECTION IV-- Criteria for Evaluation

- A. Evaluation Process
- B. PEEHIP Rights
- C. Cost and Price Analysis
- D. Proposal Evaluation Form
- E. Proposal Form

SECTION V--Attachments

- A. State of Alabama Disclosure Statement (Required by Act 2001-955)
- B. Contract Shell containing required language of State of Alabama Contracts
- C. Immigration Compliance Certificate
- D. HIPAA Business Associate Policy
- E. RSA Third Party Vendor Security Checklist--HIPAA
- F. IRS Form W-9
- G. Business Associate Agreement

SECTION I—GENERAL INFORMATION FOR THE PROPOSER

A. PURPOSE:

REQUEST FOR PROPOSALS:

The purpose of this Request for Proposals (RFP) is to solicit proposals from qualified firms to provide actuarial services to the Public Education Employees' Health Insurance Plan (PEEHIP) and the Alabama Retired Education Employees' Health Care Trust (Trust), consisting primarily of annual actuarial services for the valuation of Other Post-Employment Benefits (OPEB) for the Trust in compliance with the requirements for Governmental Accounting Standards Board (GASB) 43 and 45 and GASB 74 and 75 for the appropriate years.

B. BACKGROUND:

The Alabama Retired Education Employees' Health Care Trust (Trust) is a cost-sharing multiple-employer defined benefit postemployment healthcare plan trust that sponsors healthcare benefits to the retirees of participating state and local educational institutions. The Trust was established under the Alabama Retiree Health Care Funding Act of 2007, which was codified at Code of Alabama 1975, Sections 36-36-1 thru 36-36-11 and which authorized and directed the Public Education Employees' Health Insurance Board (Board) to create an irrevocable trust to fund postemployment healthcare benefits to retirees. Health insurance benefits for active and retired Alabama public education employees are provided through PEEHIP and paid out of the Public Education Employees' Health Insurance Fund (PEEHIF). In order to comply with the reporting requirements of GASB Statement No. 43, *Financial Reporting for Postemployment Benefit Plans Other Than Pension Plans*, the contributions and benefit payments related to retirees that are processed through the PEEHIF are segregated from the PEEHIF and reported as part of the Trust. In accordance with GASB, the Trust is considered a component unit of the State of Alabama (State) and is included in the State's Comprehensive Annual Financial Report.

PEEHIP and PEEHIF were established in 1983 by the Alabama Legislature under the provisions of Act 83-455 to provide a uniform plan of health insurance for active and retired employees of state and local educational institutions which provide instruction at any combination of grades K-14 (collectively, eligible employees), and to provide a method for funding the benefits related to the plan. The four-year universities participate in the plan with respect to their retired employees, and are eligible and may elect to participate in the plan with respect to their active employees. (At this time, only two universities have elected to participate in the plan with respect to their active employees.) Responsibility for the establishment of the health insurance plan and its general administration and operations is vested in the PEEHIP Board of Control (Board). The Board is a corporate body for purposes of management of the health insurance plan. The *Code of Alabama 1975, Section 16-25A-4* provides the Board with the authority to amend the benefit provisions in order to provide reasonable assurance of stability in future years for the plan. All assets of the Trust are held in trust for the payment of post-employment health care benefits. The Board has been appointed as the administrator of the PEEHIF and the members of the Board serve as the Trustees of the Trust.

The assets of the Trust may not be used for any purpose other than to acquire permitted investments, pay administrative expenses, and provide postemployment healthcare benefits to or for retired

employees and their dependents. The Board periodically reviews the funds available in the PEEHIF and determines if excess funds are available. If excess funds are determined to be available in the PEEHIF, the Board may authorize a transfer of funds from the PEEHIF to the Trust.

As of September 30, 2015, there were 187 participating employers and 10 participating universities in PEEHIP, and as of the latest actuarial valuation, there were 135,230 active members, 1,748 DROP members, 77,773 retired members, 24,149 participating spouses of retirees, and 1,906 participating survivors.

The PEEHIP offers a basic hospital medical plan to active members and non-Medicare eligible retirees. Benefits include inpatient hospitalization for a maximum of 365 days without a dollar limit, inpatient rehabilitation, outpatient care, physician services, and prescription drugs.

Active employees and non-Medicare eligible retirees who do not have Medicare eligible dependents can enroll in a health maintenance organization (HMO) in lieu of the basic hospital medical plan. The HMO includes hospital medical benefits, dental benefits, vision benefits, and an extensive formulary. However, participants in the HMO are required to receive care from a participating physician in the HMO plan.

The PEEHIP offers four optional plans (Hospital Indemnity, Cancer, Dental, and Vision) that may be selected in addition to or in lieu of the basic hospital medical plan or HMO. The Hospital Indemnity Plan provides a per-day benefit for hospital confinement, maternity, intensive care, cancer, and convalescent care. The Cancer Plan covers cancer disease only and benefits are provided regardless of other insurance. Coverage includes a per-day benefit for each hospital confinement related to cancer. The Dental Plan covers diagnostic and preventive services, as well as basic and major dental services. Diagnostic and preventive services include oral examinations, teeth cleaning, x-rays, and emergency office visits. Basic and major services include fillings, general aesthetics, oral surgery not covered under a Group Medical Program, periodontics, endodontics, dentures, bridgework, and crowns. Dental services are subject to a maximum of \$1,250 per year for individual coverage and \$1,000 per person per year for family coverage. The Vision Plan covers annual eye examinations, eye glasses, and contact lens prescriptions.

PEEHIP members may opt to elect the PEEHIP Supplemental Plan as their hospital medical coverage in lieu of the PEEHIP Hospital Medical Plan. The PEEHIP Supplemental Plan provides secondary benefits to the member's primary plan provided by another employer. Only active and non-Medicare retiree members and dependents are eligible for the PEEHIP Supplemental Plan. There is no premium required for this plan, and the plan covers most out-of-pocket expenses not covered by the primary plan. The plan cannot be used as a supplement to Medicare, the PEEHIP Hospital Medical Plan, or the State or Local Governmental Plans administered by the State Employees' Insurance Board (SEIB).

The *Code of Alabama 1975, Section 16-25A-8* and the *Code of Alabama 1975, Section, 16-25A-8.1* provide the Board with the authority to set the contribution requirements for plan members. Additionally, the Board is required to certify to the Governor and the Legislature the amount, as a monthly premium per active employee, necessary to fund the coverage of active and retired member benefits for the following fiscal year. The Legislature then sets the premium rate in the annual appropriation bill.

For employees who retired after September 30, 2005, but before January 1, 2012, the employer contribution of the health insurance premium set forth by the Board for each retiree class is reduced

by 2% for each year of service less than 25 and increased by 2% for each year of service over 25 subject to adjustment by the Board for changes in Medicare premium costs required to be paid by a retiree. In no case does the employer contribution of the health insurance premium exceed 100% of the total health insurance premium cost for the retiree.

For employees who retired after December 31, 2011, the employer contribution to the health insurance premium set forth by the Board for each retiree class is reduced by 4% for each year of service less than 25 and increased by 2% for each year over 25, subject to adjustment by the Board for changes in Medicare premium costs required to be paid by a retiree. In no case does the employer contribution of the health insurance premium exceed 100% of the total health insurance premium cost for the retiree. For employees who retired after December 31, 2011, who are not covered by Medicare, regardless of years of service, the employer contribution to the health insurance premium set forth by the Board for each retiree class is reduced by a percentage equal to 1% multiplied by the difference between the Medicare entitlement age and the age of the employee at the time of retirement as determined by the Board. This reduction in the employer contribution ceases upon notification to the Board of the attainment of Medicare coverage.

Each year, as noted above, the State specifies the monthly amount that participating school systems must contribute for each active employee. The monthly amount for fiscal year 2015 was \$780 per active employee. In accordance with the 2015 budget established by the Alabama Legislature, participating school systems paid the required monthly amount of \$780 on behalf of each active employee. During FY2015, \$92 million was liquidated from the Trust and used to pay retiree health care benefits. In addition to the employer payments each month, retirees are required to pay certain premium amounts. The required monthly contribution rates for fiscal year 2015 are as follows:

Retired Member Rates

- Individual Coverage/Non-Medicare Eligible - \$151
- Family Coverage/Non-Medicare Eligible Retired Member and Non-Medicare Eligible Dependent(s) - \$391
- Family Coverage/Non-Medicare Eligible Retired Member and Dependent Medicare Eligible - \$250
- Individual Coverage/Medicare Eligible Retired Member - \$10
- Family Coverage/Medicare Eligible Retired Member and Non-Medicare Eligible Dependent(s) - \$250
- Family Coverage/Medicare Eligible Retired Member and Dependent Medicare Eligible - \$109
- Tobacco surcharge - \$28 per month
- PEEHIP Supplemental Plan - \$0

-Optional Plans (Hospital Indemnity, Cancer, Dental, Vision) – up to two optional plans can be taken by retirees at no cost if the retiree is not also taking one of the Hospital Medical Plans. Otherwise, retirees can purchase the Optional Plans at the normal monthly rate of \$38 or \$45 for family dental.

-Members who retired on or after October 1, 2005, and before January 1, 2012, pay 2% of the employer premium for each year under 25 years of service, and for each year over 25 years of service, the retiree premium is reduced by 2%.

-Employees who retire on or after January 1, 2012, with less than 25 years of service, are required to pay 4% for each year under 25 years of service. Additionally, non-Medicare eligible employees who retire on or after January 1, 2012 are required to pay 1% more for each year less than age 65 (age premium) and to pay the net difference between the active employee subsidy and the non-Medicare eligible retiree subsidy (subsidy premium). When the retiree becomes Medicare eligible, the age and subsidy premiums no longer apply. However, the years of service premium (if applicable to the retiree) will continue to be applied throughout retirement. These changes are being phased in over a five-year period.

Surviving Spouse Rates

- Surviving Spouse Non-Medicare Eligible - \$700
- Surviving Spouse Non-Medicare Eligible and Dependent Non-Medicare Eligible - \$934
- Surviving Spouse Non-Medicare Eligible and Dependent Medicare Eligible - \$907
- Surviving Spouse Medicare Eligible - \$354
- Surviving Spouse Medicare Eligible and Dependent Non-Medicare Eligible - \$595
- Surviving Spouse Medicare Eligible and Dependent Medicare Eligible - \$568

C. DESCRIPTION OF THE TRUST'S MANAGEMENT:

The Trust is under the management of the Trustees of the Alabama Retired Education Employees' Health Care Trust. The Trustees, by statute, are the members of the Boards of Control of the Teachers' Retirement System of Alabama (TRS) and PEEHIP. The TRS Secretary-Treasurer is also the Chief Executive Officer (CEO) of the Trust. Several other administrative personnel are shared between TRS, PEEHIP and the Trust. This has allowed greater efficiencies by consolidating operations of the organizations by function.

D. OTHER INFORMATION:

Other documents that are considered as part of this RFP may be located via the Internet as follows:

<http://www.rsa-al.gov/index.php> - RSA home page

<http://www.rsa-al.gov/index.php/members/peehip/> -- PEEHIP Member home page

<http://www.rsa-al.gov/index.php/employers/peehip/> --PEEHIP Participating Employer home page

1. Alabama Retired Education Employees' Health Care Trust financial statements
2. Alabama Public Education Employees' Health Insurance Plan Report of Actuary on the Retiree Health Care Valuation
3. PEEHIP Publications:
 - a. Member Handbook
 - b. PEEHIP Summary Plan Description
 - c. Retirees with Medicare
 - d. PEEHIP Hospital Medical Matrix of Benefits
 - e. Supplemental Medical Plan Matrix
 - f. Optional Plan Booklet
 - g. Optional Plan Brochure
 - h. VIVA Health Plan Matrix of Benefits

E. PROPOSAL OPENING:

All proposals will be submitted (six (6) copies) in a sealed wrapper with the following plainly marked on the front:

ALABAMA RETIRED EDUCATION EMPLOYEES' HEALTH CARE TRUST (TRUST) and
PUBLIC EDUCATION EMPLOYEES' HEALTH INSURANCE PLAN

ACTUARIAL SERVICES RELATING TO HEALTHCARE COSTS AND BENEFITS INCLUDING SERVICES FOR THE VALUATION OF POST-EMPLOYMENT BENEFITS (OPEB)
RFP 16000000006
OPENING APRIL 15, 2016

Proposals will be sent to:

Via UPS or FedEx:

Diane E. Scott, CPA
Chief Financial Officer
Retirement Systems of Alabama
201 South Union Street
Montgomery, Alabama 36104-0001

Via US Mail:

Diane E. Scott
Chief Financial Officer
Retirement Systems of Alabama
PO Box 302150
Montgomery, Alabama 36130-2150

Proposals may be hand delivered to Room 792 of the Retirement Systems Building, 201 South Union Street, Montgomery, Alabama. Proposals will be accepted until 11:00 a.m. on April 15, 2016 and opened at that time. Proposals will not be accepted after this time. The PEEHIP reserves the right to reject any and all responses to this RFP. Questions related to this RFP may be addressed to Tracie Klepac at tracie.klepac@rsa-al.gov. Questions must be received by 5:00 p.m., March 8, 2016.

RFP Timetable

RFP Issued	March 1, 2016
Deadline for receipt of questions	March 8, 2016
Issue responses to questions	March 15, 2016
Proposals Due	April 15, 2016, 11:00 a.m. CST
Conduct Finalist Interviews	April 21-22, 2016
Award Contract	April 28, 2016

F. OPEB VALUATION DELIVERY SCHEDULE:

The OPEB valuations may begin for FY2015 as soon as the contract is signed by all required signatories. A final report must be completed within six weeks. In subsequent years, the OPEB valuations may begin in January and must be completed within 6 weeks.

G. PAYMENT SCHEDULE:

Payment for OPEB valuation services will be made upon the firm’s completion of the OPEB valuation and submission of written report along with a detailed invoice. Payment terms for all other actuarial services provided under this RFP shall be determined by mutual agreement of the parties.

H. SELECTION OF FIRM:

The PEEHIP expects to employ the successful Proposer to perform OPEB valuations for the fiscal years 2015-2019. All responding vendors will be notified of PEEHIP’s decision in writing within a reasonable length of time following the selection. Prior to the selection, one or more firms may be

requested to make oral presentations to the evaluation committee. All proposals shall become the property of the PEEHIP.

I. ECONOMY OF PREPARATION:

Proposals should be prepared simply and economically and provide a concise description of the Proposer's response to the requirements of this RFP. Emphasis should be on clarity. The PEEHIP will not be responsible for any costs incurred by any Proposer in the preparation of a proposal.

J. NEWS RELEASES:

News releases pertaining to this RFP or the actuarial services to which it relates will be made only with prior written approval of PEEHIP's CEO or his representative.

K. ADDENDA TO THE RFP:

Any modifications made to the RFP prior to proposal due date will be provided in writing on the PEEHIP website: <http://www.rsa-al.gov>.

L. CONTACT POINT:

Any questions that arise concerning this RFP may be directed to Tracie Klepac at tracie.klepac@rsa-al.gov.

M. MINIMUM EXPERIENCE QUALIFICATIONS:

Proposals will be accepted from firms where both the firm and the assigned lead actuarial staff members meet the following minimum experience qualifications:

- The supervising actuary must meet the American Academy of Actuaries Qualification Standards and be a Fellow of the Society of Actuaries (FSA) or an Associate of the Society of Actuaries (ASA).
- The supervising actuary should also have significant experience with public-sector retirement systems and retiree health care plans.
- The supervising actuary should have significant experience and expertise with regard to
 - Retiree health care plan design
 - OPEB accounting and reporting information under GASB Statement Nos. 43 and Statement No. 45, including implicit rate subsidies
 - Governmental funding arrangements for retiree health care
 - Medicare Part D Employer Group Waiver Plans
 - Medicare Advantage Plans
 - Industry trends in retiree health care

- Performed OPEB valuations for the most recent three (3) consecutive years of two or more public sector retiree health plans, each with at least \$200 million in premiums or claims expense and 30,000 or more retired members.

N. STATE OF ALABAMA CONTRACT REQUIREMENTS

The State of Alabama requires all providers of professional services to submit a Disclosure Statement with each contract. Accordingly, the Disclosure Statement included in Section V of this Request for Proposals (RFP) must be completed and submitted with the proposal.

The State of Alabama requires all contracts to contain certain language in a specific format. This language is outlined in the Contract shell included in Section V.

SECTION II—NATURE OF SERVICES REQUIRED

A. Purpose

The purpose of this solicitation is to acquire actuarial services for PEEHIP and the Trust, which shall initially consist primarily of OPEB valuation services for each of the 5 fiscal years ending September 30, 2015, 2016, 2017, 2018, and 2019 and ensure compliance with the reporting requirements of the Governmental Accounting Standards Board Standards Nos. 43 and 45 and any other such requirements which are announced prior to the completion of these valuations.

B. Required Services

The following services are to be provided:

1. Perform annual actuarial valuation of the ALABAMA RETIRED EDUCATION EMPLOYEES' HEALTH CARE TRUST in order to comply with GASB Nos. 43 and 45 as of the end of the fiscal year. Actuary will be provided with files detailing eligible PEEHIP members and retirees, coverage provided, and other information as required by actuary to perform the valuation. Information will be provided by the RSA Financial Accounting and Reporting Division. Valuation shall begin no later than January 1 after the end of the fiscal year and shall be completed no later than 6 weeks after January 1st except for the 2015 valuation. The 2015 valuation shall begin when the contract is fully executed and shall be completed within 6 six weeks.
2. Prepare necessary information for inclusion in the financial reports of the Alabama Retired Education Employees' Health Care Trust and/or, if applicable during the term of the engagement, the Public Education Employees' Health Insurance Plan.
3. Ensure actuarial reporting is in compliance with the requirements of the GASB pronouncements related to Other Post-Employment Benefits. We recognize that these requirements are changing during the term of this contract. Do not include costs to comply with GASB Nos. 74 and 75 in this proposal. However, the successful Proposer will work with PEEHIP to determine the implementation process and contract amendment to address these additional costs.
4. Ad hoc consulting related to OPEB or other GASB requirements.

SECTION III--INFORMATION REQUIRED FROM PROPOSERS

For any Proposal to be considered, the Proposer must submit the following information:

1. Background information of your firm including services it performs, ownership structure, the size of your firm and the location of the staff that will perform the services. Discuss in detail the services your firm performs relative to the services required of this RFP.
2. Disclose any disciplinary action or litigation taken against the firm or firm's staff regarding professional services.
3. A description of the services to be provided as described in Section II of this document including the methodologies and/or models that would be used.
4. A detailed timeline of the project identifying key phases and estimates of the hours per phase. Include expectations of client prepared workpapers and review.
5. A detailed list of data elements required along with file layouts.
6. The firm must demonstrate its experience with descriptions of three previous OPEB valuations including the plan size and a brief description of the client, name of the primary actuaries that performed the work on this project and client reference information for verification of the experience purported. These three references should be similarly situated to a plan the size of PEEHIP's retiree population. For client reference information, include contact person, e-mail, and phone number.
7. A prior OPEB valuation report compliant with GASB completed by your firm in the past twelve months.
8. A positive statement that the firm and assigned actuaries for this project have met each of the minimum qualifications set forth in Section I. M.
9. Resumes for the key personnel who will be assigned to this engagement.
10. A discussion that provides evidence of the Proposer's knowledge of the state, regional, and national healthcare market.
11. In June 2015, the Governmental Accounting Standards Board issued Statement No. 74 *Financial Reporting for Postemployment Benefit Plans Other Than Pension Plans* and Statement No. 75 *Accounting and Financial Reporting for Postemployment Benefits Other Than Pensions*. Discuss your firm's approach to implementing the changes brought about by these statements and the additional reporting that will be necessary for the actuarial firm to provide. While we recognize that the implementation guides will be released February 2017 for Statement No. 74 and November 2017 for Statement No. 75, these statements track very closely with GASB Nos. 67 and 68 for pensions. Do not include costs to comply with GASB Nos. 74 and 75 in this proposal. However, the successful Proposer will work with PEEHIP to

determine the implementation process and contract amendment to address these additional costs.

12. On December 8, 2015, the PEEHIP Board of Control adopted a Business Associate Policy. This policy is attached to this RFP. Related to this policy, please provide the following:
 - a. An statement describing your firm's ability to comply with this policy
 - b. The most recent compliance reports (external HIPAA Attestation Report or Service Organization Control Report or HITRUST certification) indicating your firm's compliance with this policy
13. Please provide a detailed transition plan for the FY 2015 OPEB valuation.
14. Please provide an overview of your firm's transition plan if the contract is not renewed in the future.
15. In Section V of this RFP is a Contract Shell with contract terms required in all State of Alabama contracts. Review this contract shell and provide an affirmative statement that Proposer will agree to the requirements for all State of Alabama contracts. In the event there are any provisions to which proposer does not agree, please provide proposed language.
16. Please provide any agreements or requirements proposer desires that PEEHIP enter into.
17. In Section V of this RFP is a copy of the PEEHIP Business Associate Agreement (BAA). Review the BAA and provide an affirmative statement that Proposer will agree to accept the terms of this BAA.
18. The cost proposal and technical proposal must be submitted in separate and clearly labeled envelopes.
19. Completion of the Proposal Form in Section IV. This cost will be used to determine the cost portion of the proposal's score.
20. The following additional forms must be completed and returned with proposal:
 - c. Vendor Disclosure Form
 - d. IRS Form W-9
 - e. Immigration Compliance Certificate
 - f. E-Verify Memorandum of Understanding issued and electronically signed by the U. S. Department of Homeland Security (note that the FEIN on the W-9 must agree with the FEIN listed on the E-Verify Memorandum)—the entire MOU should be provided
 - g. RSA Third Party Vendor Security Checklist—HIPAA
21. Include the names, e-mail addresses and telephone numbers of personnel of your organization authorized to execute the proposed contracts with the PEEHIP.
22. Include any other information believed to be pertinent but not specifically requested elsewhere in this RFP.

Section IV—Criteria for Evaluation

A. EVALUATION PROCESS

The following process will be used to evaluate vendor proposals:

- a. A review committee will evaluate by consensus scoring of each proposal submitted in response to these Proposal specifications.
- b. Responses received within the time frame and in the form specified by the guidelines will first be evaluated to confirm that all proposal sections, as detailed, have been provided in the Proposal response.
- c. Each proposal will be reviewed and points awarded to all items indicated on the Proposal Evaluation Form. Any proposal component may be awarded points not to exceed the maximum specified on the Proposal Evaluation Form. The total technical score available is 70 points.
- d. Each proposal component will be summed to obtain a total score.
- e. PEEHIP may, at its sole discretion, conduct an interview with the finalists.

B. PEEHIP'S RIGHTS

Proposers should note that PEEHIP reserves the right to modify this evaluation structure if it is deemed necessary or request additional information from vendors. It is the intention of PEEHIP to select the most qualified and cost-effective proposal based on the evaluation of the Proposer's responses to this RFP. However, PEEHIP reserves the right to ask vendors for additional information and/or an oral presentation to clarify their proposals.

C. COST AND PRICE ANALYSIS:

The cost evaluation will be based on examination by the Evaluation Committee of each Proposer's stated cost components, and will constitute 30% of the overall proposal's evaluation. The preparation of the annual valuations should be a fixed price. Billing is to be submitted with the detail by staff member of hours worked on each task. The total paid to the selected vendor for the annual valuation will not exceed the proposed cost in any fiscal year unless both parties agree.

From time to time, there may be additional requests for consulting hours outside the preparation of the annual OPEB valuation. Proposal should also provide the billing rates for consulting hours by job class.

Cost scoring will be determined as follows:

- a. Cost proposals must be provided in a separate envelope clearly labeled, "Cost Proposal".
- b. The Proposer submitting the lowest Proposal for the annual OPEB valuation will receive 25 points.
- c. The Proposer submitting the lowest average hourly consulting rates will receive 5 points.
- d. All other Proposers will be evaluated by use of the following formulae:

Lowest Cost of All Valuations
 Cost of Proposal Under Evaluation X 25 points = Proposer's Score for Cost of Valuation

Lowest Wt. Avg Cost of All Consulting Hrs.
 Wt. Avg Cost of Consulting Hrs Under Eval X 5 points = Proposer's Score for Misc Consulting Hours

NOTE: The PEEHIP will not be liable for any expense for use of any job classification by the vendor that is not identified in the vendor's response.

D. PROPOSAL EVALUATION FORM

General Proposal Categories	Possible Points	Reviewer's Score
Description of Services to be Performed	5	
Experience with Similar Proposals	20	
Experience of Personnel Assigned	20	
Knowledge of GASB 43/45 and the State, Regional and National Healthcare Market	10	
Compliance with HIPAA requirements/IT Risk	10	
Methodology (including discussion on new GASB 74 and 75 OPEB statements) and Timeline	5	
Total Technical Score	70	
Cost Proposal	30	
Total Possible Points	100	

Proposers must respond to all required components of the RFP.

E. PROPOSAL FORM

Name of Proposing Firm:

Task	Total Estimated Hours	Total Proposed Annual Valuation Cost
Annual OPEB Actuarial Valuation		

Hourly Rates and Projected Work Distribution for Assigned Staff related to OPEB valuation (this will also be the contracted rates for general consulting work):

Staff Level	Hourly Rate	Projected Distribution
Partner/Principal/Consulting Actuary	\$	
Senior Actuary	\$	
Staff Actuary	\$	
Administrative Staff	\$	
Total	N/A	100%

Ancillary expenses (travel, meals, lodging, etc.) are to be included in the proposed hourly rates.

SECTION V—Attachments

- A. State of Alabama Disclosure Statement (Required by Act 2001-955)
- B. Contract Shell containing required language of State of Alabama Contracts.
- C. Immigration Compliance Certificate
- D. HIPAA Business Associate Policy
- E. RSA Third Party Vendor Security Checklist--HIPAA
- F. IRS Form W-9
- G. Business Associate Agreement



State of Alabama Disclosure Statement

(Required by Act 2001-955)

ENTITY COMPLETING FORM

ADDRESS

CITY, STATE, ZIP

TELEPHONE NUMBER

()

STATE AGENCY/DEPARTMENT THAT WILL RECEIVE GOODS, SERVICES, OR IS RESPONSIBLE FOR GRANT AWARD

ADDRESS

CITY, STATE, ZIP

TELEPHONE NUMBER

()

This form is provided with:

Contract

Proposal

Request for Proposal

Invitation to Bid

Grant Proposal

Have you or any of your partners, divisions, or any related business units previously performed work or provided goods to any State Agency/Department in the current or last fiscal year?

Yes

No

If yes, identify below the State Agency/Department that received the goods or services, the type(s) of goods or services previously provided, and the amount received for the provision of such goods or services.

STATE AGENCY/DEPARTMENT

TYPE OF GOODS/SERVICES

AMOUNT RECEIVED

Have you or any of your partners, divisions, or any related business units previously applied and received any grants from any State Agency/Department in the current or last fiscal year?

Yes

No

If yes, identify the State Agency/Department that awarded the grant, the date such grant was awarded, and the amount of the grant.

STATE AGENCY/DEPARTMENT

DATE GRANT AWARDED

AMOUNT OF GRANT

1. List below the name(s) and address(es) of all public officials/public employees with whom you, members of your immediate family, or any of your employees have a family relationship and who may directly personally benefit financially from the proposed transaction. Identify the State Department/Agency for which the public officials/public employees work. (Attach additional sheets if necessary.)

NAME OF PUBLIC OFFICIAL/EMPLOYEE

ADDRESS

STATE DEPARTMENT/AGENCY

OVER

2. List below the name(s) and address(es) of all family members of public officials/public employees with whom you, members of your immediate family, or any of your employees have a family relationship and who may directly personally benefit financially from the proposed transaction. Identify the public officials/public employees and State Department/Agency for which the public officials/public employees work. (Attach additional sheets if necessary.)

NAME OF FAMILY MEMBER	ADDRESS	NAME OF PUBLIC OFFICIAL/ PUBLIC EMPLOYEE	STATE DEPARTMENT/ AGENCY WHERE EMPLOYED
-----------------------	---------	---	--

If you identified individuals in items one and/or two above, describe in detail below the direct financial benefit to be gained by the public officials, public employees, and/or their family members as the result of the contract, proposal, request for proposal, invitation to bid, or grant proposal. (Attach additional sheets if necessary.)

Describe in detail below any indirect financial benefits to be gained by any public official, public employee, and/or family members of the public official or public employee as the result of the contract, proposal, request for proposal, invitation to bid, or grant proposal. (Attach additional sheets if necessary.)

List below the name(s) and address(es) of all paid consultants and/or lobbyists utilized to obtain the contract, proposal, request for proposal, invitation to bid, or grant proposal:

NAME OF PAID CONSULTANT/LOBBYIST	ADDRESS
----------------------------------	---------

By signing below, I certify under oath and penalty of perjury that all statements on or attached to this form are true and correct to the best of my knowledge. I further understand that a civil penalty of ten percent (10%) of the amount of the transaction, not to exceed \$10,000.00, is applied for knowingly providing incorrect or misleading information.

Signature Date

Notary's Signature Date Date Notary Expires

Act 2001-955 requires the disclosure statement to be completed and filed with all proposals, bids, contracts, or grant proposals to the State of Alabama in excess of \$5,000.

AGREEMENT

This Agreement, which results from RFP _____ entitled Request for Proposal for _____, is made and entered into effective _____, 2016, by and between The Public Education Employees' Health Insurance Plan or "PEEHIP", and _____, hereinafter referred to as "Contractor."

SERVICES

Contractor shall provide _____ [insert description of services] to PEEHIP in accordance with the guidelines, terms and conditions set forth in PEEHIP's RFP _____ and Contractor's Proposal dated _____, all of which documents are attached hereto as Exhibit A and incorporated herein by reference.

CONSIDERATION

As consideration for the services rendered pursuant to the Agreement, PEEHIP agrees to compensate the Contractor an amount equal to the rates set forth in Contractor's Proposal. [In the alternative, edit this paragraph to clearly delineate the prices and insert maximum consideration.]

TERM

This Agreement shall be for the period beginning _____ and ending _____ . [Are there any renewal or extension options to add?]

APPROVALS

Contractor acknowledges and understands that this Agreement is not effective until it has received all required state government approvals, and Contractor shall not begin performing work under this agreement until notified to do so by PEEHIP. Contractor is entitled to no compensation for work performed prior to the effective date of this Agreement.

INDEPENDENT CONTRACTORS

Contractor acknowledges that Contractor is an independent contractor, and neither Contractor nor Contractor's employees are to be considered employees of PEEHIP or entitled to benefits under the State of Alabama Merit System.

NO STATE DEBT, ETC.

In the event of proration of the funds from which this Agreement is to be paid, the Agreement will be subject to termination by PEEHIP.

Contractor acknowledges that the terms and commitments contained herein shall not be constituted as a debt of the State of Alabama in violation of Article 11, Section 213 of the Constitution of Alabama, 1901, as amended by Amendment Number 26. It is further agreed that if any provisions of this Agreement shall contravene any statute or Constitutional provision or amendment, either now in effect or which may, during the course of this Agreement, be enacted, then that conflicting provision in the Agreement shall be deemed null and void and the remaining provisions shall continue to be valid and enforceable.

Contractor may not assign this Agreement or any interest herein or any money due hereunder without the expressed written consent of PEEHIP. Contractor's sole remedy for the settlement of any and all disputes arising under the terms of this Agreement shall be limited to the filing of a claim with the Board of Adjustment of the State of Alabama.

INDEMNIFICATION

To the fullest extent permitted by law, Contractor shall indemnify, defend, and hold harmless the Retirement Systems of Alabama, the State of Alabama, and their affiliates, and their respective administrators, officers, directors, agents, and employees (the "Indemnitees"), from and against any and all claims, damages, losses, and expenses, including but not limited to reasonable attorney's fees, arising out of or resulting from Contractor's performance of Services under this Agreement and/or any other of Contractor's acts and/or omissions under this Agreement. Without limiting the foregoing in any manner, Contractor shall indemnify, defend and hold harmless the Indemnitees from and against any and all claims, damages, losses and expenses, including but not limited to reasonable attorney's fees, (a) incurred as a result of Contractor's (or Contractor's agent's) violation of any law, rule or regulation; (b) arising out of, or related to, Contractor's (or Contractor's agent's) breach of warranty or representation; or (c) arising out of, or related to, Contractor's (or Contractor's agent's) negligent or willful misconduct. For all claims against the Indemnitees by any employee, agent, or any other person directly or indirectly employed by Contractor, the indemnification obligation under this paragraph shall not be limited in any way by any limitation on the amount or type of damages, compensation or benefits payable by or for Contractor or its agents, under worker's compensation laws, disability benefits laws or other employee benefits laws.

Contractor acknowledges and agrees that, notwithstanding anything to the contrary contained herein or in any other agreement between the parties hereto, PEEHIP shall not indemnify or hold harmless Contractor, its affiliates, administrators, officers, employees or agents. Contractor further acknowledges and agrees that PEEHIP shall not be liable to Contractor for any late fees, penalties, collection fees or attorney fees unless specifically agreed to in a writing signed by PEEHIP.

INSURANCE

Contractor agrees that Contractor shall maintain or obtain (as applicable), with respect to the activities in which Contractor engages pursuant to any Agreement that results from this RFP, general liability insurance and cyber security insurance in amounts reasonable and customary for the nature and scope of business engaged in by such party. Contractor shall deliver to PEEHIP evidence of such insurance on or before the date the Agreement goes into effect and annually thereafter.

CONFIDENTIALITY AND OWNERSHIP

Contractor acknowledges that, in the course of performing its responsibilities under this Agreement, Contractor may be exposed to or acquire information that is proprietary or confidential to PEEHIP or its members. Contractor agrees to hold such information in confidence and not to copy, reproduce, sell, assign, license, market, transfer or otherwise disclose such information to third parties or to use such information for any purpose whatsoever, without the express written permission of PEEHIP, other than for the performance of obligations hereunder or as required by applicable state or federal law. For purposes of this Agreement, all records, financial information, specifications and data disclosed to Contractor during the term of this Agreement, whether submitted orally, in writing, or by any other media, shall be deemed to be confidential in nature unless otherwise specifically stated in writing by PEEHIP.

Contractor acknowledges that all data relating to PEEHIP or PEEHIP's beneficiaries is owned by PEEHIP and constitutes valuable property of PEEHIP. PEEHIP shall retain ownership of, and all other rights and

interests with respect to, its data (including, without limitation, the content thereof, and any and all copies, modifications, alterations, and enhancements thereto, and any derivative works resulting therefrom), and nothing herein shall be construed as granting Contractor any ownership, license or any other rights of any nature with respect thereto. Contractor may not use PEEHIP's data (including de-identified data) for any purpose other than providing the Services contemplated hereunder. Upon termination of the Agreement, Contractor agrees to return or destroy all copies of PEEHIP data in its possession or control except to the extent such data must be retained pursuant to applicable law.

STATE IMMIGRATION LAW COMPLIANCE

By signing this contract, the contracting parties affirm, for the duration of the agreement, that they will not violate federal immigration law or knowingly employ, hire for employment, or continue to employ an unauthorized alien within the state of Alabama. Furthermore, a contracting party found to be in violation of this provision shall be deemed in breach of the agreement and shall be responsible for all damages resulting therefrom.

OPEN RECORDS LAW COMPLIANCE

Contractor acknowledges that PEEHIP may be subject to Alabama open records laws or similar state and/or federal laws relating to disclosure of public records and may be required, upon request, to disclose certain records and information covered by and not exempted from such laws. Contractor acknowledges and agrees that PEEHIP may comply with those laws without violating any provision of Contractor's proposal or this final Agreement. Contractor agrees to intervene in and defend any lawsuit brought against PEEHIP, the Retirement Systems of Alabama, or any of their respective employees, agent or directors, for their refusal to provide Contractor's alleged confidential and/or proprietary information to a requesting party. PEEHIP shall provide Contractor written notice of any such lawsuit within ten (10) days of receipt of service by PEEHIP. Contractor shall intervene within thirty (30) days of notice or will be deemed to have waived any and all claim that the information is confidential and/or proprietary and any and all claims against PEEHIP for disclosure of Contractor's alleged confidential and/or proprietary information.

APPLICABLE LAW

This Agreement shall be governed by and construed in accordance with Alabama Law, without giving any effect to the conflict of laws provision thereof.

TERMINATION

Termination for Convenience: This contract may be terminated for any reason by either party with the submission of a thirty (30) day written notice thereof. *[This should be contract-specific, so confirm correct timeline.]*

Termination for Default: PEEHIP may terminate immediately all or any part of a contract resulting from this proposal, by giving notice of default of PROPOSER/VENDOR, if the PROPOSER/VENDOR (1) refuses or fails to deliver the goods or services within the time specified, (2) fails to comply with any of the provisions of the Proposal or so fails to make progress as to endanger or hinder performance, (3) becomes insolvent or subject to proceedings under any law relating to bankruptcy, insolvency, or relief of debtors. In the event of termination for default, PEEHIP's liability will be limited to the payment for goods and/or services delivered and accepted as of the date of termination.

In the event of such termination or expiration of the agreement, PROPOSER/VENDOR shall return all accounts to PEEHIP, even those that are in repayment or have documented payment arrangements.

Failure To Execute Contract: Failure of the successful PROPOSER/VENDOR to enter into a contract in the time prescribed by PEEHIP may be cause for cancellation of the award to that PROPOSER/VENDOR. In the event the award is cancelled, the award may then be made to the second lowest responsible PROPOSER/VENDOR, or PEEHIP may reject all of the proposals.

ENTIRE AGREEMENT

It is understood by the parties that this instrument, including its exhibit(s), contains the entire agreement of the parties with respect to matters contained herein. No other agreement, statement or promise made by any party which is not contained in this instrument shall be binding or valid.

IN WITNESS WHEREOF, the parties have executed this Agreement effective as of the date first provided above.

Contractor Federal Tax ID Number

By: _____
Its: _____

Retirement Systems of Alabama
By: David G. Bronner
Its: Chief Executive Officer

Legally reviewed and approved by:

Legal Counsel for PEEHIP

AND

Approved by:

Governor Robert Bentley
State of Alabama

State of _____
County of _____

**CERTIFICATE OF COMPLIANCE WITH THE BEASON-HAMMON ALABAMA TAXPAYER AND CITIZEN PROTECTION ACT
(ACT 2011-535, as amended by ACT 2012-491)**

DATE: _____

RE: Contract/Grant/Incentive (describe by number or subject): _____ **by and between**

(Contractor/Grantee) and

(State Agency, Department of Public Entity)

The undersigned hereby certifies to the State of Alabama as follows:

1. The undersigned holds the position of _____ with the Contractor/Grantee named above, and is authorized to provide representations set out in this Certificate as the official and binding act of that entity, and has knowledge of the provisions of **THE BEASON-HAMMON ALABAMA TAXPAYER AND CITIZEN PROTECTION ACT** (ACT 2011-535 of the Alabama Legislature, as amended by Act 2012-491) which is described herein as "the Act".
2. Using the following definitions from Section 3 of the Act, select and initial either (a) or (b), below, to describe the Contractor/Grantee's business structure.

BUSINESS ENTITY: Any person or group of persons employing one or more persons performing or engaging in any activity, enterprise, profession, or occupation for gain, benefit, advantage, or livelihood, whether for profit or not for profit. "Business entity" shall include, but not be limited to the following:

- a. Self-employed individuals, business entities filing articles of incorporation, partnerships, limited partnerships, limited liability companies, foreign corporations, foreign limited partnerships, foreign limited liability companies authorized to transact business in this state, business trusts, and any business entity that registers with the Secretary of State.
- b. Any business entity that possesses a business license, permit, certificate, approval, registration, charter, or similar form of authorization issued by the state, any business entity that is exempt by law from obtaining such a business license and any business entity that is operating unlawfully without a business license.

EMPLOYER: Any person, firm, corporation, partnership, joint stock association, agent, manager, representative, foreman, or other person having control or custody of any employment, place of employment, or of any employee, including any person or entity employing any person for hire within the State of Alabama, including a public employer. This term shall not include the occupant of a household contracting with another person to perform casual domestic labor within the household.

___(a) the Contractor/grantee is a business entity or employer as those terms are defined in Section 3 of the Act. The Contractor/Grantee must submit its complete *E-Verify Memorandum of Understanding* issued and electronically signed by the U.S. Department of Homeland Security when the business entity or employer enrolls in the E-Verify program.

___(b) The Contractor/Grantee is not a business entity or employer as those terms are defined in Section 3 of the Act.

3. As of the date of this Certificate, Contractor/Grantee does not knowingly employ an unauthorized alien within the State of Alabama and hereafter it will not knowingly employ, hire for employment, or continue to employ an unauthorized alien within the State of Alabama;
4. Contractor/Grantee is enrolled in E-verify unless it is not eligible to enroll because of the rules of that program or other factor beyond its control.

Certified this _____ day of _____ 20 ____.

Name of Contractor/Grantee/Recipient

By:

Its:

The above Certification was signed in my presence by the person whose name appears above, on

This _____ day of _____ 20 ____.

WITNESS _____

Printed Name of Witness



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.**

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
-----------------------	--------------

Prepared By:	Title:
---------------------	---------------

Factors: Questions must be answered based on relevant systems and processes the proposed vendor will be utilizing to fulfill contract obligations in response to PEEHIP's RFP.

	I. Security Policy	YES/NO/NA	Comments
A. Policy			
1	Is there a corporate information security policy in place? If yes, provide as an attachment.		
2	Does the policy state what is and is not permissible as it pertains to sensitive company and customer information?		
3	Does the policy identify what is classified as sensitive company and customer information?		
4	Does the policy identify management and employee responsibilities including contractors?		
5	Does the policy identify use of employee owned devices such as laptops, smart phones, and any other form of device capable of storing data?		
6	Does the policy address change management requirements?		
7	Is there a policy on the portable media?(e.g., thumb drives, CDRW, etc.)		
8	Are personnel and contract personnel required to have national background check performed as part of your security policy? Please provide a copy of Proposers personnel policy if this is separate addressing hiring and termination procedures.		
B. Procedures			
1	Are procedures in place to implement the information security policy?		
2	Are the procedures and standards evaluated to determine their level of impact to the business process?		
3	Does the project management methodology uphold the security practices? If yes, explain how.		

RSA Third Party Vendor - Security Questionnaire

4	Are there policy and procedures in place to vet and audit subcontractors prior to contract acceptance where applicable?		
C. Document Handling			
1	Is there a reasonable and usable information classification policy?		
2	Does the information classification policy address all enterprise information?		
3	Is an information classification methodology in place to assist employees in identifying levels of information within the business unit?		
4	Is there an information handling matrix that explains how specific information resources are to be handled?		
II. Corporate Practices			
A. Organizational Suitability			
1	The Information Security Program has an executive level committee assigned for reporting and guidance purposes?		
2	Are employees able to perform their duties efficiently and effectively while following security procedures?		
3	Does the information security program have its' own line item in the budget?		
4	Does the security group have the authority to submit needed security policy changes throughout the enterprise?		
5	Is an annual report on the level of information security compliance issued to management?		
6	Is there more than one person responsible for the implementation of the Information Security Program?		
B. Personnel Issues			
1	Are employees able to work less than a 50 hour work week on a monthly average and complete their assignments?		
2	Are employees and project managers aware of their responsibilities for protecting information resources via written policy?		
3	Are technical employees formally trained to perform their tasks?		
4	Are contract personnel subject to confidentiality agreements?		

RSA Third Party Vendor - Security Questionnaire

5	Are contract personnel subject to the same policies employees are?		
6	Is access to sensitive/confidential information by contract personnel monitored?		
7	Are national background checks performed on all proposing party employees?		
8	Is a similar screening process carried out for contractors and temporary staff?		
9	Does employment application ask if the prospective employee has ever been convicted of a crime? If so, does proposing firm employee individuals with felony convictions?		
10	Are prior employment verifications performed for initial employment?		
11	Are there any current or pending litigations against staff, former staff, or contract staff regarding corporate espionage, identity theft, or any other areas regarding the security of privacy of confidential information?		
C. Training and Education			
1	Do employees receive security related training specific to their responsibilities? If yes, please attach a sample.		
2	Are employees receiving both positive and negative feedback related to security on their performance evaluations?		
3	Is security-related training provided periodically to reflect changes and new methods?		
4	Are system administrators given additional security training specific to their jobs?		
5	Have employees undergone a HIPAA training class for those handling personal health information (PHI) within the last year?		
D. Oversight and Auditing			
1	Is Proposer at minimum AICPA SOC 1 Type 2 compliant for financial reporting <u>for the services proposed in this RFP to PEEHIP</u> . If so, have you attached the provide the SOC report(s).		

RSA Third Party Vendor - Security Questionnaire

2	Is Proposer's datacenter where PEEHIP's data will be stored <u>for the services proposed in this RFP</u> AICPA SOC 2 Type 2 compliant? If not please comment what compliance level your datacenter facility meets.		
3	Are the security policies and procedures routinely tested?		
4	Are exceptions to security policies and procedures justified and documented?		
5	Are audit logs or other reporting mechanisms in place on all platforms?		
6	Are errors and failures tracked?		
7	When an employee is found to in non-compliance with security policies, has appropriate disciplinary action been taken?		
8	Are audits performed on an annual basis?		
9	Are unscheduled/surprise audits performed?		
10	Has someone been identified as responsible for reconciling audits?		
11	Does either an internal or external auditor independently audit Proposer's operational controls on a periodic basis?		
12	Is an independent review carried out in order to assess the effective implementation of security policies?		
13	Can the Proposer provide evidence of having gone through a recent audit of their organization's operational policies, procedures, and operating effectiveness, such as a SOC Type 2 report?		
14	Have audits been performed focusing on HIPAA, PCI, or SOX compliance? If so please, provide a copy.		
15	Has Proposer experienced a security breach of corporate or customer data within the last 10 years?		
16	Is there is any concluded or pending litigation against the Proposer or an employee related to a contract engagement or security breach?		
17	Is Proposers software solution or where data is stored compliant with HIPAA requirements?		

RSA Third Party Vendor - Security Questionnaire

18	Does Proposer have a change management committee? Does it meet on regularly scheduled intervals?		
E. Application Development and Management			
1	Has an application development methodology been implemented?		
2	Are appropriate/key application users involved with developing and improving application methodology and implementation process?		
3	Is pre-production testing performed in an isolated environment?		
4	Has a promotion to production procedures been implemented?		
5	Is there a legacy application management program?		
6	Are secure coding standards implemented and are they followed?		
7	Are applications testing for security vulnerabilities prior to being released to production?		
8	Is there a dedicated security team for testing applications for vulnerabilities?		
9	Are there procedures in place for protecting source code developed by the Proposer (physically and electronically)?		
10	Is system access and security based on the concept of least possible privilege and need-to-know?		
11	Does Proposer perform source code reviews for each release?		
12	Are backdoors prevented from being placed into application source code?		
III Physical Security			
A. Physical and Facilities where PEEHIP Data will be Stored			
1	Is access to the building(s) controlled?		
2	Is access to computing facilities where PEEHIP's data will be stored controlled more so than to the building?		
3	Is there an additional level of control for after-hours access?		
4	Is there an audit log to identify the individual and the time of access that is monitored by a group other than Information Technology?		
5	Are systems and other hardware adequately protected from theft?		
6	Are procedures in place for proper disposal of confidential information?		
7	Are proper fire suppression systems located in the facility?		

RSA Third Party Vendor - Security Questionnaire

8	Are facilities more than 5 miles from a government facility or airport?		
9	Are the servers and facilities that house software documentation and programming logic located in a secure facility?		
10	Is all confidential and restricted information marked as such and stored in a secure area (room, cabinet) with access restricted to authorized personnel only?		
11	Does Proposer allow employees to work remote or in a virtual environment? Please provide documentation around controls for safeguarding computer systems and confidential data.		
B. After-Hours Review			
1	Are areas containing sensitive information properly secured?		
2	Are workstation secured after-hours?		
3	Are keys and access cards properly secured?		
4	Is confidential information properly secured?		
5	Are contract cleaning crews activities monitored?		
C. Incident Handling			
1	Has an Incident Response Team (IRT) been established?		
2	Have employees been trained as to when the IRT should be notified?		
3	Has the IRT been trained in evidence gathering and handling?		
4	Are incident reports issued to appropriate management?		
5	After an incident, are policies and procedures reviewed to determine if modification need to be implemented?		
6	Does the Proposer have a process in place to notify IT security of breaches and/or problems so that proper notification and correction can be done?		
D. Contingency Planning			
1	Has a Business Impact Analysis been conducted on all systems, applications, and platforms?		
2	Is there a documented data center Disaster Recovery Plan (DRP) in place?		
3	Are backup media password protected or encrypted?		

RSA Third Party Vendor - Security Questionnaire

4	Has the data center DRP been tested within the past 12 months?		
5	Are system, application, and data backups sent to a secure off-site facility on a regular basis?		
6	Are Service Level Agreements that identify processing requirements in place with all users and service providers?		
7	Have departments, business units, groups, and other such entities implemented business continuity plans that supplement the data center DRP?		
8	Have Emergency Response Procedures (ERP) been implemented?		
9	Have ERPs been tested for effectiveness?		
IV. Business Impact Analysis, Disaster Recovery Plan			
A. General Review			
1	Backup planning includes identification of all critical data, programs, documentation, and support items required performing essential task during recovery?		
2	The BIA is reviewed and updated regularly with special attention to new technology, business changes, and migration of applications to alternative platforms?		
3	Critical period timeframes have been identified for all applications and systems?		
4	Senior management has reviewed and approved the prioritized list of critical applications?		
B. Disaster Recovery Plan (DRP)			
1	A corporate disaster recovery plan coordinator has been named and a mission statement identifying scope and responsibilities has been published?		
2	A "worst-case" scenario DRP to recover normal operations within the prescribed timeframes has been implemented and tested?		
3	Listing of current emergency telephone numbers for police, fire department, medical aid, and company officials are strategically located throughout the facility and at off-site locations?		

RSA Third Party Vendor - Security Questionnaire

4	The backup site is remote from hazards that endanger the main data center?		
5	Contracts for outsourced activities have been amended to include service providers' responsibilities for DRP?		
6	Lead times for communication lines and equipment, specialized devices, power hookups, construction, firewalls, computer configurations, and LAN implementation have been factored into the DRP?		
7	At least one copy of the DRP is stored at the backup site and is updated regularly?		
8	Automatic restart and recovery procedures are in place to restore data files in the event of a processing failure?		
9	Contingency arrangements are in place for hardware, software, communications, software, staff and supplies.		
10	Customer software solutions that are being developed and/or in production are backed up as part of the Proposer's backup and recovery procedures?		
C. Testing			
1	Backup and recovery procedures are tested at least annually?		
2	Training sessions are conducted for all relevant personnel on backup, recovery, and contingency operating procedures?		
3	Appropriate user representative have a particular role in creating and reviewing control reliability and backup provisions for relevant applications?		
4	Appropriate user representatives participate in the DRP tests?		
Other Issues			
1	Provisions are in place to maintain the security of processing functions in the event of an emergency?		
2	Insurance coverage for loss of hardware and business impact is in place?		
V. Technical Safeguards			
A. Passwords			

RSA Third Party Vendor - Security Questionnaire

1	Are host systems and servers as well as application servers secured with unique passwords?		
2	Are default accounts de-activated?		
3	Are temporary user accounts restricted and disabled within 4 hours?		
4	Are the password management systems forcing users to change passwords every 90 days or less?		
5	Are users of all company-provided network resources required to change the initial default password?		
6	Are the passwords complex? Contain upper case, lower case, special character or number, and at least 8 characters long.		
7	Do network and system administrators have adequate experience to implement security standards?		
8	Are reports and logs pertaining to network users reviewed and reconciled on a regular basis?		
9	Are permissions being set securely?		
10	Are administrators assigned a unique ID for access to critical systems?		
11	Are administrators using appropriate tools to perform their jobs?		
12	Does the application support multi-factor authentication?		
13	Are online systems always secured using SSL encryption?		
B. Infrastructure			
1	Is the network infrastructure audited on an annual basis?		
2	Are network vulnerability assessments conducted on an annual basis?		
3	Are changes/improvements made in a timely fashion following network vulnerability assessments?		
4	If you house or develop solutions around credit card transactions are you CISP compliant?		
C. Firewalls			
1	Are protocols allowed to initiate connections from "outside" the firewall?		

RSA Third Party Vendor - Security Questionnaire

2	Has a risk analysis been conducted to determine if the protocols allowed maintain an acceptable level of risk?		
3	Has the firewall been tested to determine if outside penetration is possible?		
4	Are other products in place to augment the firewall level security?		
5	Are the firewalls maintained and monitored 24x7?		
6	Have services offered across the firewall been documented?		
7	Has a Demilitarized Zone (DMZ) or Perimeter Network been implemented?		
8	Has the firewall administrator been formally trained?		
9	Is there more than one person administering the firewall?		
10	Is the firewall for the ASP separate from the corporate firewall?		
D. Data Communications			
1	Is there a remote access procedure in place?		
2	Is there a current network diagram?		
3	Are Access Control List (ACLs) maintained on a regular basis?		
4	Is the network environment partitioned?		
5	Are the corporate routers separated from the ASP routers?		
6	Are the corporate switches separated from the ASP switches?		
7	Does the communication equipment log administrative access to the systems?		
8	Is SNMP data collected from the data communication devices?		
9	Is syslog data collected from the data communication devices?		
10	Are there standard templates for configuring routers?		
11	Are there standard templates for configuring switches?		
E. Databases			
1	Are default database passwords changed?		
2	Are database administrators trained or certified?		
3	Are database backups performed daily?		
F. Computing Platforms			
1	Are critical servers protected with appropriate access controls?		
2	Are development staff administrators on their computers used for writing source code?		

RSA Third Party Vendor - Security Questionnaire

3	Is there a company image used for corporate PCs and laptops?		
4	Does the company have an asset management system to track software installed?		
5	Is there an anti-virus application installed on all PC's, laptops, and servers?		
6	Does the anti-virus application automatically update computing assets 3 times or more per day?		
7	Is there a URL filtering solution in place?		
8	Do computing assets have a corporate anti-malware application installed?		
9	Are Internet facing servers protected with host based intrusion prevention?		
10	Are employees restricted to what can be installed on their computer systems? How is this managed for remote employees if applicable?		
11	Do any of the Proposer's computer systems including storage reside on a cloud computing environment? Is it owned and operated by the Proposer? If no, please explain.		
G. Intrusion Prevention			
1	Is host based intrusion prevention software installed on all Internet facing servers?		
2	Are network based intrusion prevention systems in-line and defending?		
3	Is host based intrusion prevention software installed on all laptops?		
4	Is there a dedicated security staff monitoring 24x7 alerts from the host based intrusion prevention?		
5	Is there a dedicated security staff monitoring 24x7 alerts from the network based intrusion prevention?		
VI. Telecommunications Security			
A. Policy			
1	Is there a published policy on the use of organizational telecommunications resources?		

RSA Third Party Vendor - Security Questionnaire

2	Have all employees have been made aware of the telecommunications policy?		
3	Employees authorized for Internet access are made aware of the organization's proprietary information and what they can discuss in open forums?		
4	Employees using cellular or wireless phones are briefed on the lack of privacy of conversations when using unsecured versions of technology?		
5	The organization has a published policy on prosecution of employees and outsiders if found guilty of serious premeditated criminal acts against the organization?		
6	Are corporate devices such as iPhones or Android based phones centrally managed by the Proposer to control rogue software installations and protect corporate data?		
B. Standards			
1	A threshold is established to monitor and suspend repeated unsuccessful dial-in or remote access attempts?		
2	Access to databases reachable via dial-in or VPN have access control in place to prevent unauthorized access?		
3	Financial applications available via dial-in or VPN have audit trails established to track access and transaction usage?		
4	Are audit trails reviewed and corrective action taken on a regular basis?		
5	When possible are acl security programs used to control dial-in or remote access to a specific application?		
6	Company proprietary data, stored on portable computers are secured from unauthorized access?		
7	Are corporate emails allowed to be sent from unique domains not one used by Proposer such as Gmail or Microsoft Email?		
8	Users of all company-provided communication systems are required to change the default or initial password?		
C. Practices			

Request for Taxpayer Identification Number and Certification

**Give Form to the
requester. Do not
send to the IRS.**

Print or type See Specific Instructions on page 2.	1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.	
	2 Business name/disregarded entity name, if different from above	
	3 Check appropriate box for federal tax classification; check only one of the following seven boxes: <input type="checkbox"/> Individual/sole proprietor or single-member LLC <input type="checkbox"/> C Corporation <input type="checkbox"/> S Corporation <input type="checkbox"/> Partnership <input type="checkbox"/> Trust/estate <input type="checkbox"/> Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=partnership) ▶ _____ Note. For a single-member LLC that is disregarded, do not check LLC; check the appropriate box in the line above for the tax classification of the single-member owner. <input type="checkbox"/> Other (see instructions) ▶ _____	4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3): Exempt payee code (if any) _____ Exemption from FATCA reporting code (if any) _____ <i>(Applies to accounts maintained outside the U.S.)</i>
	5 Address (number, street, and apt. or suite no.)	Requester's name and address (optional)
	6 City, state, and ZIP code	
	7 List account number(s) here (optional)	

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the Part I instructions on page 3. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN* on page 3.

Note. If the account is in more than one name, see the instructions for line 1 and the chart on page 4 for guidelines on whose number to enter.

Social security number											
				-			-				
OR											
Employer identification number											
				-							

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions on page 3.

Sign Here	Signature of U.S. person ▶	Date ▶
------------------	----------------------------	--------

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.
Future developments. Information about developments affecting Form W-9 (such as legislation enacted after we release it) is at www.irs.gov/fw9.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following:

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)

- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding? on page 2.

By signing the filled-out form, you:

1. Certify that the TIN you are giving is correct (or you are waiting for a number to be issued),
2. Certify that you are not subject to backup withholding, or
3. Claim exemption from backup withholding if you are a U.S. exempt payee. If applicable, you are also certifying that as a U.S. person, your allocable share of any partnership income from a U.S. trade or business is not subject to the withholding tax on foreign partners' share of effectively connected income, and
4. Certify that FATCA code(s) entered on this form (if any) indicating that you are exempt from the FATCA reporting, is correct. See *What is FATCA reporting?* on page 2 for further information.

Note. If you are a U.S. person and a requester gives you a form other than Form W-9 to request your TIN, you must use the requester's form if it is substantially similar to this Form W-9.

Definition of a U.S. person. For federal tax purposes, you are considered a U.S. person if you are:

- An individual who is a U.S. citizen or U.S. resident alien;
- A partnership, corporation, company, or association created or organized in the United States or under the laws of the United States;
- An estate (other than a foreign estate); or
- A domestic trust (as defined in Regulations section 301.7701-7).

Special rules for partnerships. Partnerships that conduct a trade or business in the United States are generally required to pay a withholding tax under section 1446 on any foreign partners' share of effectively connected taxable income from such business. Further, in certain cases where a Form W-9 has not been received, the rules under section 1446 require a partnership to presume that a partner is a foreign person, and pay the section 1446 withholding tax. Therefore, if you are a U.S. person that is a partner in a partnership conducting a trade or business in the United States, provide Form W-9 to the partnership to establish your U.S. status and avoid section 1446 withholding on your share of partnership income.

In the cases below, the following person must give Form W-9 to the partnership for purposes of establishing its U.S. status and avoiding withholding on its allocable share of net income from the partnership conducting a trade or business in the United States:

- In the case of a disregarded entity with a U.S. owner, the U.S. owner of the disregarded entity and not the entity;
- In the case of a grantor trust with a U.S. grantor or other U.S. owner, generally, the U.S. grantor or other U.S. owner of the grantor trust and not the trust; and
- In the case of a U.S. trust (other than a grantor trust), the U.S. trust (other than a grantor trust) and not the beneficiaries of the trust.

Foreign person. If you are a foreign person or the U.S. branch of a foreign bank that has elected to be treated as a U.S. person, do not use Form W-9. Instead, use the appropriate Form W-8 or Form 8233 (see Publication 515, Withholding of Tax on Nonresident Aliens and Foreign Entities).

Nonresident alien who becomes a resident alien. Generally, only a nonresident alien individual may use the terms of a tax treaty to reduce or eliminate U.S. tax on certain types of income. However, most tax treaties contain a provision known as a "saving clause." Exceptions specified in the saving clause may permit an exemption from tax to continue for certain types of income even after the payee has otherwise become a U.S. resident alien for tax purposes.

If you are a U.S. resident alien who is relying on an exception contained in the saving clause of a tax treaty to claim an exemption from U.S. tax on certain types of income, you must attach a statement to Form W-9 that specifies the following five items:

1. The treaty country. Generally, this must be the same treaty under which you claimed exemption from tax as a nonresident alien.
2. The treaty article addressing the income.
3. The article number (or location) in the tax treaty that contains the saving clause and its exceptions.
4. The type and amount of income that qualifies for the exemption from tax.
5. Sufficient facts to justify the exemption from tax under the terms of the treaty article.

Example. Article 20 of the U.S.-China income tax treaty allows an exemption from tax for scholarship income received by a Chinese student temporarily present in the United States. Under U.S. law, this student will become a resident alien for tax purposes if his or her stay in the United States exceeds 5 calendar years. However, paragraph 2 of the first Protocol to the U.S.-China treaty (dated April 30, 1984) allows the provisions of Article 20 to continue to apply even after the Chinese student becomes a resident alien of the United States. A Chinese student who qualifies for this exception (under paragraph 2 of the first protocol) and is relying on this exception to claim an exemption from tax on his or her scholarship or fellowship income would attach to Form W-9 a statement that includes the information described above to support that exemption.

If you are a nonresident alien or a foreign entity, give the requester the appropriate completed Form W-8 or Form 8233.

Backup Withholding

What is backup withholding? Persons making certain payments to you must under certain conditions withhold and pay to the IRS 28% of such payments. This is called "backup withholding." Payments that may be subject to backup withholding include interest, tax-exempt interest, dividends, broker and barter exchange transactions, rents, royalties, nonemployee pay, payments made in settlement of payment card and third party network transactions, and certain payments from fishing boat operators. Real estate transactions are not subject to backup withholding.

You will not be subject to backup withholding on payments you receive if you give the requester your correct TIN, make the proper certifications, and report all your taxable interest and dividends on your tax return.

Payments you receive will be subject to backup withholding if:

1. You do not furnish your TIN to the requester,
2. You do not certify your TIN when required (see the Part II instructions on page 3 for details),

3. The IRS tells the requester that you furnished an incorrect TIN,

4. The IRS tells you that you are subject to backup withholding because you did not report all your interest and dividends on your tax return (for reportable interest and dividends only), or

5. You do not certify to the requester that you are not subject to backup withholding under 4 above (for reportable interest and dividend accounts opened after 1983 only).

Certain payees and payments are exempt from backup withholding. See *Exempt payee code* on page 3 and the separate instructions for the Requester of Form W-9 for more information.

Also see *Special rules for partnerships* above.

What is FATCA reporting?

The Foreign Account Tax Compliance Act (FATCA) requires a participating foreign financial institution to report all United States account holders that are specified United States persons. Certain payees are exempt from FATCA reporting. See *Exemption from FATCA reporting code* on page 3 and the Instructions for the Requester of Form W-9 for more information.

Updating Your Information

You must provide updated information to any person to whom you claimed to be an exempt payee if you are no longer an exempt payee and anticipate receiving reportable payments in the future from this person. For example, you may need to provide updated information if you are a C corporation that elects to be an S corporation, or if you no longer are tax exempt. In addition, you must furnish a new Form W-9 if the name or TIN changes for the account; for example, if the grantor of a grantor trust dies.

Penalties

Failure to furnish TIN. If you fail to furnish your correct TIN to a requester, you are subject to a penalty of \$50 for each such failure unless your failure is due to reasonable cause and not to willful neglect.

Civil penalty for false information with respect to withholding. If you make a false statement with no reasonable basis that results in no backup withholding, you are subject to a \$500 penalty.

Criminal penalty for falsifying information. Willfully falsifying certifications or affirmations may subject you to criminal penalties including fines and/or imprisonment.

Misuse of TINs. If the requester discloses or uses TINs in violation of federal law, the requester may be subject to civil and criminal penalties.

Specific Instructions

Line 1

You must enter one of the following on this line; **do not** leave this line blank. The name should match the name on your tax return.

If this Form W-9 is for a joint account, list first, and then circle, the name of the person or entity whose number you entered in Part I of Form W-9.

a. **Individual.** Generally, enter the name shown on your tax return. If you have changed your last name without informing the Social Security Administration (SSA) of the name change, enter your first name, the last name as shown on your social security card, and your new last name.

Note. ITIN applicant: Enter your individual name as it was entered on your Form W-7 application, line 1a. This should also be the same as the name you entered on the Form 1040/1040A/1040EZ you filed with your application.

b. **Sole proprietor or single-member LLC.** Enter your individual name as shown on your 1040/1040A/1040EZ on line 1. You may enter your business, trade, or "doing business as" (DBA) name on line 2.

c. **Partnership, LLC that is not a single-member LLC, C Corporation, or S Corporation.** Enter the entity's name as shown on the entity's tax return on line 1 and any business, trade, or DBA name on line 2.

d. **Other entities.** Enter your name as shown on required U.S. federal tax documents on line 1. This name should match the name shown on the charter or other legal document creating the entity. You may enter any business, trade, or DBA name on line 2.

e. **Disregarded entity.** For U.S. federal tax purposes, an entity that is disregarded as an entity separate from its owner is treated as a "disregarded entity." See Regulations section 301.7701-2(c)(2)(iii). Enter the owner's name on line 1. The name of the entity entered on line 1 should never be a disregarded entity. The name on line 1 should be the name shown on the income tax return on which the income should be reported. For example, if a foreign LLC that is treated as a disregarded entity for U.S. federal tax purposes has a single owner that is a U.S. person, the U.S. owner's name is required to be provided on line 1. If the direct owner of the entity is also a disregarded entity, enter the first owner that is not disregarded for federal tax purposes. Enter the disregarded entity's name on line 2, "Business name/disregarded entity name." If the owner of the disregarded entity is a foreign person, the owner must complete an appropriate Form W-8 instead of a Form W-9. This is the case even if the foreign person has a U.S. TIN.

Line 2

If you have a business name, trade name, DBA name, or disregarded entity name, you may enter it on line 2.

Line 3

Check the appropriate box in line 3 for the U.S. federal tax classification of the person whose name is entered on line 1. Check only one box in line 3.

Limited Liability Company (LLC). If the name on line 1 is an LLC treated as a partnership for U.S. federal tax purposes, check the "Limited Liability Company" box and enter "P" in the space provided. If the LLC has filed Form 8832 or 2553 to be taxed as a corporation, check the "Limited Liability Company" box and in the space provided enter "C" for C corporation or "S" for S corporation. If it is a single-member LLC that is a disregarded entity, do not check the "Limited Liability Company" box; instead check the first box in line 3 "Individual/sole proprietor or single-member LLC."

Line 4, Exemptions

If you are exempt from backup withholding and/or FATCA reporting, enter in the appropriate space in line 4 any code(s) that may apply to you.

Exempt payee code.

- Generally, individuals (including sole proprietors) are not exempt from backup withholding.
- Except as provided below, corporations are exempt from backup withholding for certain payments, including interest and dividends.
- Corporations are not exempt from backup withholding for payments made in settlement of payment card or third party network transactions.
- Corporations are not exempt from backup withholding with respect to attorneys' fees or gross proceeds paid to attorneys, and corporations that provide medical or health care services are not exempt with respect to payments reportable on Form 1099-MISC.

The following codes identify payees that are exempt from backup withholding. Enter the appropriate code in the space in line 4.

1—An organization exempt from tax under section 501(a), any IRA, or a custodial account under section 403(b)(7) if the account satisfies the requirements of section 401(f)(2)

2—The United States or any of its agencies or instrumentalities

3—A state, the District of Columbia, a U.S. commonwealth or possession, or any of their political subdivisions or instrumentalities

4—A foreign government or any of its political subdivisions, agencies, or instrumentalities

5—A corporation

6—A dealer in securities or commodities required to register in the United States, the District of Columbia, or a U.S. commonwealth or possession

7—A futures commission merchant registered with the Commodity Futures Trading Commission

8—A real estate investment trust

9—An entity registered at all times during the tax year under the Investment Company Act of 1940

10—A common trust fund operated by a bank under section 584(a)

11—A financial institution

12—A middleman known in the investment community as a nominee or custodian

13—A trust exempt from tax under section 664 or described in section 4947

The following chart shows types of payments that may be exempt from backup withholding. The chart applies to the exempt payees listed above, 1 through 13.

IF the payment is for . . .	THEN the payment is exempt for . . .
Interest and dividend payments	All exempt payees except for 7
Broker transactions	Exempt payees 1 through 4 and 6 through 11 and all C corporations. S corporations must not enter an exempt payee code because they are exempt only for sales of noncovered securities acquired prior to 2012.
Barter exchange transactions and patronage dividends	Exempt payees 1 through 4
Payments over \$600 required to be reported and direct sales over \$5,000 ¹	Generally, exempt payees 1 through 5 ²
Payments made in settlement of payment card or third party network transactions	Exempt payees 1 through 4

¹See Form 1099-MISC, Miscellaneous Income, and its instructions.

²However, the following payments made to a corporation and reportable on Form 1099-MISC are not exempt from backup withholding: medical and health care payments, attorneys' fees, gross proceeds paid to an attorney reportable under section 6045(f), and payments for services paid by a federal executive agency.

Exemption from FATCA reporting code. The following codes identify payees that are exempt from reporting under FATCA. These codes apply to persons submitting this form for accounts maintained outside of the United States by certain foreign financial institutions. Therefore, if you are only submitting this form for an account you hold in the United States, you may leave this field blank. Consult with the person requesting this form if you are uncertain if the financial institution is subject to these requirements. A requester may indicate that a code is not required by providing you with a Form W-9 with "Not Applicable" (or any similar indication) written or printed on the line for a FATCA exemption code.

A—An organization exempt from tax under section 501(a) or any individual retirement plan as defined in section 7701(a)(37)

B—The United States or any of its agencies or instrumentalities

C—A state, the District of Columbia, a U.S. commonwealth or possession, or any of their political subdivisions or instrumentalities

D—A corporation the stock of which is regularly traded on one or more established securities markets, as described in Regulations section 1.1472-1(c)(1)(i)

E—A corporation that is a member of the same expanded affiliated group as a corporation described in Regulations section 1.1472-1(c)(1)(i)

F—A dealer in securities, commodities, or derivative financial instruments (including notional principal contracts, futures, forwards, and options) that is registered as such under the laws of the United States or any state

G—A real estate investment trust

H—A regulated investment company as defined in section 851 or an entity registered at all times during the tax year under the Investment Company Act of 1940

I—A common trust fund as defined in section 584(a)

J—A bank as defined in section 581

K—A broker

L—A trust exempt from tax under section 664 or described in section 4947(a)(1)

M—A tax exempt trust under a section 403(b) plan or section 457(g) plan

Note. You may wish to consult with the financial institution requesting this form to determine whether the FATCA code and/or exempt payee code should be completed.

Line 5

Enter your address (number, street, and apartment or suite number). This is where the requester of this Form W-9 will mail your information returns.

Line 6

Enter your city, state, and ZIP code.

Part I. Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. If you are a resident alien and you do not have and are not eligible to get an SSN, your TIN is your IRS individual taxpayer identification number (ITIN). Enter it in the social security number box. If you do not have an ITIN, see *How to get a TIN* below.

If you are a sole proprietor and you have an EIN, you may enter either your SSN or EIN. However, the IRS prefers that you use your SSN.

If you are a single-member LLC that is disregarded as an entity separate from its owner (see *Limited Liability Company (LLC)* on this page), enter the owner's SSN (or EIN, if the owner has one). Do not enter the disregarded entity's EIN. If the LLC is classified as a corporation or partnership, enter the entity's EIN.

Note. See the chart on page 4 for further clarification of name and TIN combinations.

How to get a TIN. If you do not have a TIN, apply for one immediately. To apply for an SSN, get Form SS-5, Application for a Social Security Card, from your local SSA office or get this form online at www.ssa.gov. You may also get this form by calling 1-800-772-1213. Use Form W-7, Application for IRS Individual Taxpayer Identification Number, to apply for an ITIN, or Form SS-4, Application for Employer Identification Number, to apply for an EIN. You can apply for an EIN online by accessing the IRS website at www.irs.gov/businesses and clicking on Employer Identification Number (EIN) under Starting a Business. You can get Forms W-7 and SS-4 from the IRS by visiting IRS.gov or by calling 1-800-TAX-FORM (1-800-829-3676).

If you are asked to complete Form W-9 but do not have a TIN, apply for a TIN and write "Applied For" in the space for the TIN, sign and date the form, and give it to the requester. For interest and dividend payments, and certain payments made with respect to readily tradable instruments, generally you will have 60 days to get a TIN and give it to the requester before you are subject to backup withholding on payments. The 60-day rule does not apply to other types of payments. You will be subject to backup withholding on all such payments until you provide your TIN to the requester.

Note. Entering "Applied For" means that you have already applied for a TIN or that you intend to apply for one soon.

Caution: A disregarded U.S. entity that has a foreign owner must use the appropriate Form W-8.

Part II. Certification

To establish to the withholding agent that you are a U.S. person, or resident alien, sign Form W-9. You may be requested to sign by the withholding agent even if items 1, 4, or 5 below indicate otherwise.

For a joint account, only the person whose TIN is shown in Part I should sign (when required). In the case of a disregarded entity, the person identified on line 1 must sign. Exempt payees, see *Exempt payee code* earlier.

Signature requirements. Complete the certification as indicated in items 1 through 5 below.

1. Interest, dividend, and barter exchange accounts opened before 1984 and broker accounts considered active during 1983. You must give your correct TIN, but you do not have to sign the certification.

2. Interest, dividend, broker, and barter exchange accounts opened after 1983 and broker accounts considered inactive during 1983. You must sign the certification or backup withholding will apply. If you are subject to backup withholding and you are merely providing your correct TIN to the requester, you must cross out item 2 in the certification before signing the form.

3. Real estate transactions. You must sign the certification. You may cross out item 2 of the certification.

4. Other payments. You must give your correct TIN, but you do not have to sign the certification unless you have been notified that you have previously given an incorrect TIN. "Other payments" include payments made in the course of the requester's trade or business for rents, royalties, goods (other than bills for merchandise), medical and health care services (including payments to corporations), payments to a nonemployee for services, payments made in settlement of payment card and third party network transactions, payments to certain fishing boat crew members and fishermen, and gross proceeds paid to attorneys (including payments to corporations).

5. Mortgage interest paid by you, acquisition or abandonment of secured property, cancellation of debt, qualified tuition program payments (under section 529), IRA, Coverdell ESA, Archer MSA or HSA contributions or distributions, and pension distributions. You must give your correct TIN, but you do not have to sign the certification.

What Name and Number To Give the Requester

For this type of account:	Give name and SSN of:
1. Individual	The individual
2. Two or more individuals (joint account)	The actual owner of the account or, if combined funds, the first individual on the account ¹
3. Custodian account of a minor (Uniform Gift to Minors Act)	The minor ²
4. a. The usual revocable savings trust (grantor is also trustee) b. So-called trust account that is not a legal or valid trust under state law	The grantor-trustee ¹ The actual owner ¹
5. Sole proprietorship or disregarded entity owned by an individual	The owner ³
6. Grantor trust filing under Optional Form 1099 Filing Method 1 (see Regulations section 1.671-4(b)(2)(i)(A))	The grantor*
For this type of account:	Give name and EIN of:
7. Disregarded entity not owned by an individual	The owner
8. A valid trust, estate, or pension trust	Legal entity ⁴
9. Corporation or LLC electing corporate status on Form 8832 or Form 2553	The corporation
10. Association, club, religious, charitable, educational, or other tax-exempt organization	The organization
11. Partnership or multi-member LLC	The partnership
12. A broker or registered nominee	The broker or nominee
13. Account with the Department of Agriculture in the name of a public entity (such as a state or local government, school district, or prison) that receives agricultural program payments	The public entity
14. Grantor trust filing under the Form 1041 Filing Method or the Optional Form 1099 Filing Method 2 (see Regulations section 1.671-4(b)(2)(i)(B))	The trust

¹ List first and circle the name of the person whose number you furnish. If only one person on a joint account has an SSN, that person's number must be furnished.

² Circle the minor's name and furnish the minor's SSN.

³ You must show your individual name and you may also enter your business or DBA name on the "Business name/disregarded entity" name line. You may use either your SSN or EIN (if you have one), but the IRS encourages you to use your SSN.

⁴ List first and circle the name of the trust, estate, or pension trust. (Do not furnish the TIN of the personal representative or trustee unless the legal entity itself is not designated in the account title.) Also see *Special rules for partnerships* on page 2.

*Note. Grantor also must provide a Form W-9 to trustee of trust.

Note. If no name is circled when more than one name is listed, the number will be considered to be that of the first name listed.

Secure Your Tax Records from Identity Theft

Identity theft occurs when someone uses your personal information such as your name, SSN, or other identifying information, without your permission, to commit fraud or other crimes. An identity thief may use your SSN to get a job or may file a tax return using your SSN to receive a refund.

To reduce your risk:

- Protect your SSN,
- Ensure your employer is protecting your SSN, and
- Be careful when choosing a tax preparer.

If your tax records are affected by identity theft and you receive a notice from the IRS, respond right away to the name and phone number printed on the IRS notice or letter.

If your tax records are not currently affected by identity theft but you think you are at risk due to a lost or stolen purse or wallet, questionable credit card activity or credit report, contact the IRS Identity Theft Hotline at 1-800-908-4490 or submit Form 14039.

For more information, see Publication 4535, Identity Theft Prevention and Victim Assistance.

Victims of identity theft who are experiencing economic harm or a system problem, or are seeking help in resolving tax problems that have not been resolved through normal channels, may be eligible for Taxpayer Advocate Service (TAS) assistance. You can reach TAS by calling the TAS toll-free case intake line at 1-877-777-4778 or TTY/TDD 1-800-829-4059.

Protect yourself from suspicious emails or phishing schemes. Phishing is the creation and use of email and websites designed to mimic legitimate business emails and websites. The most common act is sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

The IRS does not initiate contacts with taxpayers via emails. Also, the IRS does not request personal detailed information through email or ask taxpayers for the PIN numbers, passwords, or similar secret access information for their credit card, bank, or other financial accounts.

If you receive an unsolicited email claiming to be from the IRS, forward this message to phishing@irs.gov. You may also report misuse of the IRS name, logo, or other IRS property to the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484. You can forward suspicious emails to the Federal Trade Commission at: spam@uce.gov or contact them at www.ftc.gov/idtheft or 1-877-IDTHEFT (1-877-438-4338).

Visit IRS.gov to learn more about identity theft and how to reduce your risk.

Privacy Act Notice

Section 6109 of the Internal Revenue Code requires you to provide your correct TIN to persons (including federal agencies) who are required to file information returns with the IRS to report interest, dividends, or certain other income paid to you; mortgage interest you paid; the acquisition or abandonment of secured property; the cancellation of debt; or contributions you made to an IRA, Archer MSA, or HSA. The person collecting this form uses the information on the form to file information returns with the IRS, reporting the above information. Routine uses of this information include giving it to the Department of Justice for civil and criminal litigation and to cities, states, the District of Columbia, and U.S. commonwealths and possessions for use in administering their laws. The information also may be disclosed to other countries under a treaty, to federal and state agencies to enforce civil and criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. You must provide your TIN whether or not you are required to file a tax return. Under section 3406, payers must generally withhold a percentage of taxable interest, dividend, and certain other payments to a payee who does not give a TIN to the payer. Certain penalties may also apply for providing false or fraudulent information.

BUSINESS ASSOCIATE AGREEMENT

This Agreement is made and entered into this ____ day of _____, 20__, by and between _____ (“Business Associate”) and the Public Education Employees’ Health Insurance Board (“Plan Sponsor”), acting on behalf of the Public Education Employees’ Health Insurance Plan (“Covered Entity”). This Agreement is incorporated within the Services Agreement entered into by and between Business Associate and the Public Education Employees’ Health Insurance Plan as of the ____ day of _____, 20__.

WHEREAS, Business Associate and Covered Entity desire and are committed to complying with all relevant federal and state laws with respect to the confidentiality and security of Protected Health Information (PHI), including, but not limited to, the federal Health Insurance Portability and Accountability Act of 1996, and accompanying regulations, as amended from time to time (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and any regulations promulgated thereunder.

NOW, THEREFORE, for valuable consideration the receipt of which is hereby acknowledged and intending to establish a business associate relationship under 45 CFR §164, the parties hereby agree as follows:

I. Definitions

- A. “Business Associate” shall have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean _____.
- B. “Breach” shall be defined as set out in 45 CFR §164.402.
- C. “CFR” means the Code of Federal Regulations. A reference to a CFR section means that section as amended from time to time; provided that if future amendments change the designation of a section referred to herein, or transfer a substantive regulatory provision referred to herein to a different section, the section references herein shall be deemed to be amended accordingly.
- D. “Compliance Date(s)” shall mean the date(s) established by the Secretary or the United States Congress as the effective date(s) of applicability and enforceability of the Privacy Rule, Security Rule and HITECH Standards.
- E. “Designated Record Set” shall have the same meaning as the term “designated record set” in 45 CFR §164.501 and shall include a group of records that is: (i) the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for Covered Entity by Business Associate or (2) used, in whole or in part, by or for Covered Entity to make decisions about Individuals.
- F. “Electronic Protected Health Information” (EPHI) shall have the same meaning as the term “electronic protected health information” in 45 CFR §160.103, limited to the information received from or created on behalf of Covered Entity by Business Associate.
- G. “HITECH Standards” shall mean the privacy, security and security breach notification provisions applicable to a Business Associate under Subtitle D of the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009, as such law may be amended from time to time, and any regulations promulgated thereunder.

- H. "Individual" shall have the same meaning as the term "individual" in 45 CFR §160.103, and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
- I. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160 and 164, subparts A and E.
- J. "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in 45 CFR §160.103, limited to the information received from or created on behalf of Covered Entity by Business Associate.
- K. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR §164.501.
- L. "Security Incident" shall have the same meanings as the term "security incident" in 45 CFR §164.304.
- M. "Security Rule" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR parts 160 and 164, subparts A and C.
- N. "Unsecured PHI" shall have the same meaning as "unsecured protected health information" in 45 CFR §164.402.

Terms used, but not otherwise defined, shall have the same meaning as those terms in the Privacy Rule, Security Rule and HITECH Standards.

II. Obligations of Business Associate

- A. Business Associate agrees not to use or disclose PHI other than as permitted or required by this Agreement or as Required by Law. Business Associate will take reasonable efforts to limit requests for, use and disclosure of PHI to the minimum necessary to accomplish the intended request, use or disclosure and comply with 45 CFR §§ 164.502(b) and 514(d) .
- B. To the extent the Business Associate conducts a "Standard Transaction" as outlined in 45 CFR Part 162, Business Associate agrees to comply and to require any agent or subcontractor to comply with all applicable requirements set forth in 45 CFR Part 162.
- C. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement. Business Associate shall implement administrative, physical, and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule.
- D. Business Associate agrees to report to Covered Entity any use or disclosure of PHI other than as provided for by this Agreement promptly after Business Associate has actual knowledge of such use or disclosure, and to report promptly to the Covered Entity all Security Incidents of which it becomes aware. Following the discovery of a Breach of Unsecured PHI, Business Associate shall notify Covered Entity of such Breach without unreasonable delay, and in no event later than 30 calendar days after such discovery. The notification will include the identification of each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed during the Breach. A Breach shall be treated as discovered as of the first day on which such Breach is known or reasonably should have been known to Business Associate. The

parties acknowledge and agree that this section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity is required by applicable laws or regulations. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI, and so long as additional notice to Covered Entity is not required by applicable laws or regulations.

- E. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable regulations. Business Associate has a duty to assist the Covered Entity in any mitigation, notice, reporting, or other remedial actions required, all of which would be at the Covered Entity's request and in the Covered Entity's sole discretion.
- F. Business Associate agrees to include in its agreement with any agent or subcontractor to whom it provides PHI on behalf of the Covered Entity conditions with respect to such information that are at least as restrictive as those that apply through this Agreement to Business Associate. Business Associate agrees to ensure that any agents, including sub-agents, to whom it provides EPHI received from, or created or received by Business Associate on behalf of the Covered Entity, agree in writing to implement the same reasonable and appropriate safeguards that apply to Business Associate to protect the Covered Entity's EPHI.
- G. If Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to make available to Covered Entity, within a reasonable time, such information as Covered Entity may require to fulfill Covered Entity's obligations to respond to a request for access to PHI as provided under 45 CFR §164.524 or to respond to a request to amend PHI as required under 45 CFR §164.526. Business Associate shall refer to Covered Entity all such requests that Business Associate may receive from Individuals. If Covered Entity requests Business Associate to amend PHI in Business Associate's possession in order to comply with 45 CFR §164.526, Business Associate shall effectuate such amendments no later than the date they are required to be made by 45 CFR §164.526; provided that if Business Associate receives such a request from Covered Entity less than ten (10) business days prior to such date, Business Associate will effectuate such amendments as soon as is reasonably practicable.
- G. If applicable, Business Associate agrees to provide to Covered Entity within a reasonable time such information necessary to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures as provided under 45 CFR §164.528. Business Associate shall refer to Covered Entity all such requests which Business Associate may receive from Individuals.
- H. Upon reasonable notice, Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the U.S. Secretary of Health and Human Services, or an officer or employee of that Department to whom relevant authority has been delegated, at Covered Entity's expense in a reasonable time and manner, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- I. Notwithstanding any other provision in this Agreement, Business Associate hereby acknowledges and agrees that to the extent it is functioning as a Business Associate of Covered Entity, Business Associate will comply with the HITECH Business Associate provisions and with the obligations of a Business Associate as prescribed by HIPAA and the HITECH Act commencing on the Compliance Date of each such provision. Business Associate and the Covered Entity further agree

that the provisions of HIPAA and the HITECH Act that apply to Business Associates and that are required to be incorporated by reference in a Business Associate Agreement are incorporated into this Agreement between Business Associate and Covered Entity as if set forth in this Agreement in their entirety and are effective as of the Compliance Date.

III. Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this Agreement, Business Associate may:

- A. Use or disclose Protected Health Information on behalf of the Covered Entity, if such use or disclosure of Protected Health Information would not violate the Privacy Rule, including the minimum necessary standard, if done by the Covered Entity.
- B. Use or disclose PHI to perform the services outlined in the <applicable services agreement>.
- C. Use Protected Health Information for the proper management and administration of Business Associate or to fulfill any present or future legal responsibilities of Business Associate.
- D. Disclose Protected Health Information for the proper management and administration of Business Associate or to fulfill any present or future legal responsibilities of Business Associate, provided that such disclosure is either Required by Law or Business Associate obtains reasonable assurances from any person to whom Protected Health Information is disclosed that such person will: (i) keep such information confidential, (ii) use or further disclose such information only for the purpose for which it was disclosed to such person or as Required by Law, and (iii) notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- E. Use Protected Health Information to provide data aggregation services relating to the health care operations of the Covered Entity, as provided in 45 CFR §164.501.
- F. To create de-identified data, provided that the Business Associate de-identifies the information in accordance with the Privacy Rule. De-identified information does not constitute PHI and is not subject to the terms and conditions of this Agreement.
- G. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).
- H. Business Associate agrees to ensure that access to EPHI related to the Covered Entity is limited to those workforce members who require such access because of their role or function. Business Associate agrees to implement safeguards to prevent its workforce members who are not authorized to have access to such EPHI from obtaining access and to otherwise ensure compliance by its workforce with the Security Rule.

IV. Obligations of Covered Entity

- A. Covered Entity shall notify Business Associate of any facts or circumstances that affect Business Associate's use or disclosure of PHI. Such facts and circumstances include, but are not limited to: (i) any limitation or change in Covered Entity's notice of privacy practices, (ii) any changes in, or withdrawal of, an authorization provided to Covered Entity by an Individual pursuant to 45 CFR §164.508; and (iii) any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522.

- B. Covered Entity warrants that it will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or is not otherwise authorized or permitted under this Agreement.
- C. Covered Entity acknowledges and agrees that the Privacy Rules allow the Covered Entity to permit Business Associate to disclose or provide access to PHI, other than Summary Health Information, to the Plan Sponsor only after the Plan Sponsor has amended its plan documents to provide for the permitted and required uses and disclosures of PHI and to require the Plan Sponsor to provide a certification to the Plan that certain required provisions have been incorporated into the Plan documents before the Plan may disclose, either directly or through a Business Associate, any PHI to the Plan Sponsor. Covered Entity hereby warrants and represents that Plan documents have been so amended and that the Plan has received such certification from the Plan Sponsor.
- D. Covered Entity agrees that it will have entered into Business Associate Agreements with any third parties to whom Covered Entity directs and authorizes Business Associate to disclose PHI.

V. Effective Date; Termination

- A. The effective date of this Agreement shall be the date this Agreement is signed by both parties (or the Compliance Date, if later).
- B. This Agreement shall terminate on the date Business Associates ceases to be obligated to perform the functions, activities, and services described in Article III.
- C. Upon Covered Entity's knowledge of a material breach or violation of this Agreement by Business Associate, Covered Entity shall notify Business Associate of such breach or violation and Business Associate shall have thirty (30) days to cure the breach or end the violation. In the event Business Associate does not cure the breach or end the violation, Covered Entity shall have the right to immediately terminate this Agreement and any underlying services agreement if feasible.
- D. INTENTIONALLY OMITTED.
- E. Upon termination of this Agreement, Business Associate will return to Covered Entity, or if return is not feasible, destroy, any and all PHI that it created or received on behalf of Covered Entity and retain no copies thereof. If the return or destruction of the PHI is determined by Business Associate not to be feasible, Business Associate shall limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. If return or destruction of the PHI is feasible but Business Associate is required by law to retain such information or copies thereof, Business Associate will maintain the PHI for the period of time required under applicable law after which time Business Associate shall return or destroy the PHI.
- F. Business Associate's obligations under Sections II and III of this Agreement shall survive the termination of this Agreement with respect to any PHI so long as it remains in the possession of Business Associate.

VI. Other Provisions

- A. The parties acknowledge that the foregoing provisions are designed to comply with the mandates of the Privacy and Security Rules and the HITECH Standards and agree to make any necessary changes to this agreement that may be required by any amendment to the final regulations promulgated by the Secretary. If the parties are unable to reach agreement regarding an amendment

within thirty (30 days) of the date that Business Associate receives any written objection from Covered Entity, either party may terminate this Agreement upon ninety (90) days written notice to the other party. Any other amendment to the Agreement unrelated to compliance with applicable law and regulations shall be effective only upon execution of a written agreement between the parties.

- B. Except as it relates to the use, security and disclosure of PHI and electronic transactions, this Agreement is not intended to change the terms and conditions of, or the rights and obligations of the parties under any other services agreement between them.
- C. Business Associate agrees to defend, indemnify and hold harmless Covered Entity, its affiliates and each of their respective directors, officers, employees, agents or assigns from and against any and all actions, causes of action, claims, suits and demands whatsoever, and from all damages, liabilities, costs, charges, debts, fines, government investigations, proceedings, and expenses whatsoever (including reasonable attorneys' fees and expenses related to any litigation or other defense of any claims), which may be asserted or for which they may now or hereafter become subject arising in connection with (i) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of Business Associate under this Agreement; and (ii) any claims, demands, awards, judgments, actions, and proceedings made by any person or organization arising out of or in any way connected with Business Associate's performance under this Agreement.
- D. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
- E. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Entity to comply with the Privacy and Security Rules and the HITECH Standards.
- F. If any provision of this Agreement is held illegal, invalid, prohibited or unenforceable by a court of competent jurisdiction, that provision shall be limited or eliminated in that jurisdiction to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.
- G. This Agreement replaces and supersedes in its (their) entirety any prior Business Associate Agreement(s) between the parties.

[SIGNATURE PAGE TO FOLLOW]

IN WITNESS WHEREOF, this Agreement has been signed and delivered as of the date first set forth above.

**Public Education Employees' Health Insurance Board,
the Plan Sponsor, acting on behalf of Covered Entity**

<Business Associate>

Signature

Signature

Printed Name

Printed Name

Title

Title