Request for Proposal

Special Investigation Unit (SIU) Services

Solicitation Number: ARFP PEI2700000001

TECHNICAL PROPOSAL

West Virginia Public Employees Insurance Agency

RFP Release Date: September 25, 2026

RFP Due Date: November 13, 2026

Contract Effective Date: January 1, 2027

TABLE OF CONTENTS

SECTION 1	**General Information and Instructions**
SECTION 2	**Instructions to Vendors Submitting Bids**
SECTION 3	**General Terms and Conditions**
SECTION 4	**Agency & Project Information**
SECTION 5	**Mandatory Requirements**
SECTION 6	**Technical Response Questions**
SECTION 7	**Vendor Proposal**
SECTION 8	**Evaluation and Award**
SECTION 9	**Vendor Attachments to Include with Bid**
SECTION 10	**RFP Attachments**
SECTION 11	**Vendor Signature and Certification**

SECTION 1: GENERAL INFORMATION AND INSTRUCTIONS

1.1. Introduction:

The West Virginia Public Employees Insurance Agency (the PEIA or the Agency) is issuing this solicitation as a request for proposal ("RFP") to seek bids from qualified Vendors to provide post- payment claim review services such as recognizing and flagging member eligibility and provider billing abnormalities indicative of fraud, waste, or abuse; identifying, investigating and recovering overpayments; collaborating with the Agency's Third Party Administrator (TPA) to implement prepayment reviews of claims submitted by providers identified as outliers to prevent improper payments; and collaborating with the Agency's Pharmacy Benefit Manager (PBM) to implement post-payment processes to reduce and recover improper payments more effectively and efficiently.

The RFP is a procurement method in which vendors submit proposals in response to the request for proposal published by the Purchasing Division. It requires an award to the highest scoring vendor, rather than the lowest cost vendor, based upon a technical evaluation of the vendor's technical proposal and a cost evaluation. This is referred to as a best value procurement. Through their proposals, vendors offer a solution to the objectives, problem, or need specified in the RFP, and define how they intend to meet (or exceed) the RFP requirements.

This procurement is exempt from some requirements of the West Virginia Purchasing Division pursuant to W. Va. Code §5A-3-10b.

This Agency administers electronic protected health information (PHI). PEIA is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

1.2. Vendor Understanding

By signing and submitting its proposal, the Vendor agrees to be bound by all the terms contained in this Request for Proposal (RFP). An RFP is generally used for the procurement of services in situations where price is not the sole determining factor and the award will be based on a combination of cost and technical factors ("Best Value"). Through its proposal, the Vendor offers a solution to the objectives, problem, or need specified in the RFP, and defines how it intends to meet (or exceed) the RFP requirements.

1.3 RFP Schedule of Events (All dates subject to change if necessary)

RFP Issued	September 25, 2026
Vendor Question Deadline	October 9, 2026
PEIA Responses Deadline	October 23, 2026
Vendor Bids Due	November 13, 2026
Finalist Interviews (Oral Presentation)	TBD
BAFO (optional)	TBD
Expected Award Date	December 1, 2026
Final Vendor Documents Received	10 days following award date
Expected Contract Finalization	30 days following award date

SECTION 2: INSTRUCTIONS TO VENDORS SUBMITTING BIDS

2.1 Review Documents Thoroughly

The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid. PEIA is not responsible for any misinterpretation by the Vendor of the terms and conditions of this RFP.

2.2 Mandatory Terms

The Solicitation contains mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

2.3 Vendor Question Deadline

Vendors may submit questions relating to this solicitation to the WV Public Employees Insurance Agency. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below in order to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are non-binding.

Submitted emails should have the solicitation number in the subject line.

Question Submission Deadline: ***October 9, 2026, by 5:00 pm EDT***

Submit Questions to:	**Sam Revercomb**
Physical Address:	**601 57th Street SE, Suite 2, Charleston, WV 25304**
Fax:	**1-877-233-4295**
Email:	**Samuel.H.Revercomb@wv.gov**

2.4 Bid Submission

All bids must be signed and delivered by the Vendor to the Agency on or before the date and time of the bid opening. Any bid received by the Agency staff is considered to be in the possession of the Agency and will not be returned for any reason. Acceptable delivery methods include hand delivery, delivery by courier or Postal carrier, or email. PEIA is not responsible for any delays in delivery created by any third party, i.e. courier, U.S. Postal Service, e-mail server or application, etc.

2.4.1 Two-Part Submission: Vendors must submit two distinct proposals: a Technical Proposal and a Cost Proposal. Technical proposals must not contain any cost

information relating to the project. Cost proposals must be in the format of the Cost Proposal Workbook provided.

2.4.2 Scoring Summary: The Technical proposal is separate from the Cost proposal and must not contain any mention of the pricing contained in the Cost proposal. However, information such as labor hours and categories, materials, subcontracts, and so forth, shall be contained in the Technical Proposal so that the Bidder's understanding of the scope of the work may be evaluated. The Technical Proposal shall disclose the Bidder's technical approach in as much detail as possible, including, but not limited to, the information required by the Technical Proposal instructions.

Proposing entities will be eligible to move forward for Cost proposal evaluation if they obtain a minimum acceptable score for the service(s) they propose. The minimum acceptable score for the Technical Proposal will be set at 70% or 42 points.

The sum of the scores for each of the criteria will constitute 60% of the overall evaluation criteria, based on a total available score of 60 points. The raw scores will then be averaged to obtain a composite score. Any proposal with less than 42 of the potential 60 points for technical ability will be disqualified.

The Cost proposal criteria will be evaluated in terms of absolute dollars and will constitute 40% of the overall evaluation criteria. Each proposed contract price will be evaluated by using the following formula:

Cost Evaluation Formula: Each Cost proposal will have points assigned using the following formula for all Vendors not disqualified during the Technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1: Lowest Cost of All Proposals / Cost of Proposal Being Evaluated = Cost Score Percentage

Step 2: Cost Score Percentage X Points Allocated to Cost Proposal = **Total Cost Score**

Example:

Proposal 1 Cost is $1,000,000

Proposal 2 Cost is $1,100,000

Points Allocated to Cost Proposal is 40

Proposal 1: Step 1 – $1,000,000 / $1,000,000 = Cost Score Percentage of 1 (100%)

Step 2 – 1 X 40 = Total Cost Score of 40

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091

(90.9091%)
Step 2 – 0.909091 X 40 = Total Cost Score of 36.36364

After the Technical proposal and Cost proposal evaluation have been performed, the two scores will be added together to constitute the final score for each proposal.

Points Available

Technical Proposal	**60 Points**
Cost Proposal	**40 Points**
Total Score	**100 Points**

2.4.3 Required: One (1) searchable electronic copy of EACH proposal. Cost and Technical proposals must be prepared as separate documents and submitted separately: as separate, clearly marked electronic files; as separate, clearly marked digital media; or as separate, clearly marked emails.

2.4.4 Electronic File Access Restrictions: Vendor must ensure that electronic submissions can be accessed and viewed immediately after the bid due date. The Agency will consider any file that cannot be immediately accessed and viewed (such as encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires, and therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after the bid due date to make a file viewable.

The email address for electronic bid delivery is:

Samuel.H.Revercomb@wv.gov

Proposing company must submit proposals as follows:

REQUIRED: One (1) searchable electronic copy of EACH proposal (Cost and Technical proposals must be prepared as separate documents and submitted as separate files).

Bids should contain the information listed below in the body of each email and on the face of each physical proposal. Bids submitted without this information may be rejected by the Agency.

Note: Items in italics are for informational purposes only as a means of assisting Vendor in marking their bid submissions.

SEALED BID: *Service/Commodity*
SOLICITATION NUMBER: *Document Number from Solicitation*

VENDOR INFORMATION:	*Vendor Name, Address, and Telephone Number*
CONTACT:	*Primary Vendor Contact Name*
PROPOSAL TYPE:	*Technical Proposal or Cost Proposal*

2.5 Addendum Acknowledgment

Changes or revisions to this Solicitation will be made by an official written addendum issued by the PEIA. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing Attachment 16 (Addendum Acknowledgement Form**). Failure to acknowledge addenda may result in bid disqualification.** The addendum acknowledgement should be submitted with the bid to expedite document processing.

2.6 Bid Formatting

Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification. The bid should be clear and concise; no more than 75 pages with a minimum 10-point font; all pages must be numbered sequentially; including a response to each listed mandatory term and condition; with any references to attachments or appendices clearly marked. **The question must be restated prior to all responses. Failure to restate the questions may be terms for disqualification.**

2.7 Exceptions and Clarifications

The Solicitation contains the project specifications, vendor requirements, and terms and conditions that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. The PEIA is under no obligation to consider or negotiate any terms and conditions or alternative terms and conditions contained in the Vendor's proposals. If PEIA rejects an exception, clarification, or proposed modification and Vendor cannot accept the original term or requirement as stated in the RFP and its attachments, Vendor may be disqualified.

> **NOTE**: A vendor may not request an exception, clarification, or modification to circumvent a mandatory minimum requirement.

2.8 Communication Limitations

Communication with the PEIA about this solicitation is limited to the Solicitation contact during the solicitation, bid, evaluation, or award periods without prior approval by the Solicitation contact. This provision is not intended to restrict current contractors from communicating with PEIA staff regarding ongoing operational matters.

2.9 Vendor State Registration

Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the $125 fee, if applicable. Vendors may find information at:

http://www.state.wv.us/admin/purchase/VendorReg.html

2.10 Unit Price

Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

2.11 Waiver of Minor Irregularities

The PEIA Director reserves the right to waive minor irregularities in bids or specifications.

2.12 Non-Responsible Bid

The PEIA Director or designee reserves the right to reject the bid of any vendor as *non-responsible* when it is determined that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance.

2.13 RFP/RFQ Withdrawal, Modification, and Cancellation

The PEIA may withdraw, cancel, or modify an RFP/RFQ at any time. Submission of proposals or receipt of proposals by the PEIA confer no rights upon the Vendor and do not obligate the PEIA in any manner. Further, the PEIA may accept or reject any bid in whole, or in part.

Proposals must be valid for 180 days following the close date of this RFP. This period may be extended by written mutual agreement between the Bidder and WV PEIA.

2.14 Small, Women-Owned, Or Minority-Owned Businesses

Small, Women-Owned, Or Minority-Owned Businesses: For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37 and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women- owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors.

2.15 Interested Party Disclosure

West Virginia § 6D-1-2 requires that the vendor submit to PEIA a disclosure of interested parties to the contract for all contracts with an actual or estimated value of at least $1 Million prior to finalization of the contract. That disclosure must occur on the form prescribed and approved by the WV Ethics Commission prior to contract award. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above. A copy of that form is available from the Agency Buyer designated in Section 2.4 above.

2.16 Mandatory Responses / Attachments

Vendor is responsible for ensuring that any item listed in the specification as a Mandatory Response or Mandatory Attachment is included with the initial bid submission. **Failure to include Mandatory Responses or Mandatory Attachments will result in bid disqualification.**

2.17 Additional Documentation Or Information After Bid Submission

In instances where these specifications require documentation or information not listed as a Mandatory Response or Mandatory Attachment, or PEIA needs additional information to clarify or verify a vendor response, PEIA reserves the right to request those items after bid opening and prior to contract award. **This does not apply to instances where State law mandates receipt with the bid.** When PEIA sends a request, the vendor will be provided a timeframe within to provide the requested information. **Failure to provide the information or documentation within the timeframe provided could result in disqualification.**

Example: The Data Management Addendum is required before the contract is finalized but is not a Mandatory Attachment. If the vendor does not provide a signed copy with their bid and PEIA determines that it is not otherwise disqualified, the Vendor will receive a request for a signed Data Management Addendum within a certain number of days. Failure to do so will result in disqualification.

2.18 Public Document: This RFP, any bid proposals, and any resulting contract is subject to public disclosure under the West Virginia Freedom of Information Act ("FOIA"). Bidders must agree and understand that their submissions may be subject to disclosure or release based on a FOIA request. Accordingly, if the Bidder considers any part of its bid proposal to contain "proprietary," "confidential," "private," or "trade secret" information exempt from disclosure under FOIA then the Bidder must provide a second, redacted copy of its bid proposal in conjunction with the original bid proposal. **If no redacted copy of a Bid submission is received from the Bidder, the PEIA is compelled by law to release the unredacted bid submission to a FOIA requester.** For what may be viewed as exempt from disclosure under FOIA, please see W. Va. Code § 29B-1-4(a)(1) here:

http://www.wvlegislature.gov/WVCODE/ChapterEntire.cfm?chap=29B&art=1&section=4#01

For purposes of redaction, the vendor must be specific as to why a FOIA exemption applies. Redactions must be "surgical" and not "global", i.e. redaction of the number(s) after a percentage (%) or a price ($) mark and not redactions of whole paragraphs or pages. If a FOIA request is received, or the released redacted version is challenged by the requestor, the PEIA will notify the Bidder in writing via e-mail of the request and provide them a copy of the FOIA submission. Bidders shall assume all responsibilities for the defense in a Court of competent jurisdiction of the non-release of their Bid submission under the FOIA statutes. The PEIA assumes no liability for defending any release under FOIA nor can it assist in, act on behalf of, nor represent a Bidder in such a defense. For additional information on how a "trade secret" is defined under West Virginia law, see W. Va. Code § 47-22-1(d) here:

http://www.wvlegislature.gov/WVCODE/ChapterEntire.cfm?chap=47&art=22&section=1#22#22

As the PEIA is an entity of West Virginia State government, this RFP and any bid proposals, as well as any resulting contract, are subject to audit, inspection, and review by entities within West Virginia State government including, but not limited to the West Virginia Department of Administration, the West Virginia Division of Purchasing, the West Virginia Attorney General's Office, and the West Virginia Legislature. The PEIA shall not be responsible for any subsequent release or disclosures made by State entities outside of the Agency.

2.19 Best and Final Offer: Best and Final Offer (BAFO) may be requested as part of this process from responsive and responsible proposals received. (Note: PEIA reserves the right to make a contract award without any further discussion with potential Bidders regarding the proposals received. Therefore, proposals should be submitted initially on the most favorable terms available to PEIA from a cost and technical standpoint).

SECTION 3: GENERAL TERMS AND CONDITIONS

By submitting a bid for this procurement, the vendor agrees to the terms and conditions of this solicitation including, but not limited to, all vendor responsibilities, required submissions, and further agrees and understands that the terms and conditions of this solicitation shall constitute the material basis of the contract between the Agency and the vendor. This RFP may contain mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification. Should the vendor, for any reason, take exception to a term or condition listed in this solicitation, it is their responsibility to:

a. Cite the specific term or condition to which they take exception;
b. Provide a detailed explanation of their stated exception; and
c. Proffer a viable alternative to the cited term or condition.

PEIA reserves the right to reject exceptions requested by prospective vendors.

3.1 Contractual Agreement

Once a vendor has been notified that they are the apparent successful bidder, PEIA and the Vendor will compile a final contract document that incorporates the Request for Proposal, the Vendor's Proposal, and any relevant required documentation. The contract is considered "executed" when both entities have signed the final contract document.

3.2 Definitions - As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

3.2.1 "Agency" means the Public Employees Insurance Agency (PEIA)

3.2.2 **"Award Document"** means the document completed in the State's system which records the contract with the State and ensures it can be paid.

3.2.3 **"Bid"** or **"Proposal"** means the response submitted by the vendor to this solicitation.

3.2.4 **"Business Associate"** means any person or entity as defined by 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e) of HIPAA. The Vendor for this contract shall be considered a Business Associate of the Agency.

3.2.5 **"Business Associate Agreement"** or **"WV BAA"** means the State of West Virginia Executive Branch Business Associate Agreement and corresponding Appendix A which are incorporated by reference to the terms and conditions of this RFP and subsequent contract, if awarded. See Attachment 8.

3.2.6 **"Contract"** means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

3.2.7 **"Data Management Addendum"** or **"WV DMA"** means the State of West Virginia Executive Branch Data Management Addendum which is incorporated by reference to the terms and conditions of this RFP and subsequent contract, if awarded. See Attachment 7.

3.2.8 **"Director"** means the Director of the West Virginia Public Employees Insurance Agency

3.2.9 **"Exempt"** means the solicitation/purchase is exempt from the requirements of the West Virginia Dept. of Administration Purchasing Division as designated in W. Va. Code §5A-3-10b.

3.2.10 **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191,and its implementing regulations codified at 45 CFR Parts 160, 162, and 164, inclusive of the Privacy, Security, Breach Notification, and Enforcement Rules, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the HIPAA Omnibus Final Rule of 2013.

3.2.11 **"HITECH"** means the Health Information Technology for Economic and Clinical Health Act of 2009 adopted as part of the American Recovery and Reinvestment Act (ARRA).

3.2.12 **"NIST"** means the National Institute of Standards and Technology" specifically as it relates to HIPAA compliance as outlined in NIST SP 800-53, Revision 5; NIST SP-800-66, Revision 2; and NIST SP 800-88 Revision 2, including any active updates, errata, or successor revisions issued during the contract lifecycle.

3.2.13 **"ROI"** means Return on Investment reflected as a ratio of dollars spent to dollars saved in healthcare expenditures.

3.2.14 "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Public Employment Insurance Agency.

3.2.15 "Vendor" or **"Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the highest scoring responsible bidder, or the entity that has been awarded the Contract as context requires.

3.2.16 "Abuse" means medical practices that are inconsistent with sound fiscal, business, or medical practices that result in an unnecessary cost to the PEIA health care plans, or in reimbursement for services that are not medically necessary or fail to meet professional recognized standards for health care.

3.2.17 "FWA" means Fraud, Waste and Abuse

3.2.18 "Fraud" means the intentional deception or misrepresentation made by a person with the knowledge that deception could result in some unauthorized benefit to himself or some other person. It includes any act that constitutes fraud under applicable federal or state law.

3.2.19 "Waste" means the overutilization of resources or practices that result in inappropriate payment.

3.2.20 "Third Party Administrator" (otherwise known as a 'TPA') means a business organization that performs administrative services for PEIA such as billing, plan design, claims processing, record keeping, and regulatory compliance activities in connection with medical and other healthcare services received by its members.

3.2.21 "Pharmacy Benefits Manager" (otherwise known as a 'PBM') means a person, business, or other entity that performs pharmacy benefits management for PEIA, as defined in West Virginia Code §33-51-3.

3.2.22 "Prepayment Review" means the evaluation of claims *prior* to payment adjudication to identify billing errors, abnormalities, or potential FWA, resulting in the denial or modification of the claim before state funds are disbursed.

3.2.23 "Post-payment Review" means the retrospective auditing and analysis of paid claims data to identify overpayments, billing abnormalities, or patterns of FWA, followed by recovery actions for improperly disbursed funds.

3.2.24 "Overpayment" means any payment made to a provider or pharmacy benefits manager by the Agency, TPA, or PBM that exceeds the amount that is legally, contractually, or clinically due.

3.2.25 "Algorithm" or "Edit" means the proprietary or customized electronic data rules, predictive models, machine learning parameters, or statistical screens used by the Vendor to scan claims and identify outliers or abnormalities.

3.2.26 "Contingency Fee" means a pricing structure wherein the Vendor's compensation is a contractually agreed-upon percentage of actual overpayments successfully recovered and returned to the Agency.

3.2.27 "**Shared Savings Model"** means a value-based compensation framework where the Vendor is remunerated based on a percentage of the total, validated financial reductions achieved for the Agency. These savings are calculated against an established historical expenditure baseline and encompass both "Hard Recoveries" (cash clawed back through retrospective post-payment audits) and "Hard Cost Avoidance" (claims successfully blocked or corrected prior to adjudication via prepayment reviews).

3.3 Contract Term: Renewal

The term of this Contract shall be as follows:

Term Contract

This Contract is anticipated to be signed and fully executed by December 15, 2026.* Project launch is anticipated to be no later than January 1, 2027* and the contract is anticipated to terminate on December 31, 2029.* It is IMPERATIVE the vendor review and submit signed documents in a timely manner.

(* Dates subject to change as necessary).

Renewal Term

This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Automatic renewal of this Contract is prohibited.

Incorporation by Reference

The terms and conditions of this solicitation shall be incorporated by reference into and shall be considered binding in the final contract.

3.4 Notice to Proceed

Unless otherwise specified, the signed, fully executed contract will be considered notice to proceed.

3.5 Quantities

The quantities required under this Contract are determined in accordance with the category(ies) identified as applicable to this Contract:

Open End Contract

Quantities listed in this Solicitation/Final Contract are approximations only, based on estimates supplied by PEIA. It is understood and agreed that the Contract shall cover actual quantities during the term of the Contract, whether more or less than the quantities shown.

Services

The scope of the services to be provided will be more clearly defined in the specifications included herewith.

3.6 Emergency Purchases

The PEIA Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the PEIA Director, shall not constitute a breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One Time Purchase contract.

3.7 Insurance

The apparent successful Vendor shall furnish proof of the insurance identified by a mark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendors must also provide the Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancellation, policy reduction, or change in insurers.

The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether or not that insurance requirement is listed in this section.

Vendor must maintain:

[X] **Comprehensive General Liability Insurance** applicable to the services provided to PEIA, with a combined single limit, or the equivalent, of not less than $5,000,000 for each occurrence or not less than $10,000,000 in the aggregate. For Errors and Omissions, Bodily Injury, Personal Injury, and Property Damage, including contractual liability coverage applicable to the indemnity provided under this contract.

[X] **Automobile Liability Insurance** in at least an amount of: $1,000,000 per occurrence. "Policy must include coverage for all owned, leased, hired, and non-owned automobiles used in connection with the performance of this Contract."

[X] **Professional/Malpractice/Errors and Omission Insurance** applicable to the services provided to PEIA, of not less than $5,000,000 for each occurrence or not less than $10,000,000 in the aggregate.

[ ] Commercial Crime and Third Party Fidelity Insurance in an amount of: $_____ per occurrence.

[X] **Cyber Liability Insurance** of not less than $5,000,000 for each occurrence or not less than $10,000,000 in the aggregate. Said cyber policy must include the coverage(s) for any and/or all subcontractors who may perform any, part, some, or all of the work on the proposed contract..

[ ] _____

[ ] _____

3.8 Workers' Compensation Insurance

The apparent successful Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

3.9 Acceptance

Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

3.10 Pricing

The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification.

3.11 Payment in Arrears

Payment in advance is prohibited under this Contract. Payment may only be made after the delivery and acceptance of goods or services. The Vendor shall submit invoices in arrears.

3.12 Payment Terms

Payment in advance is prohibited under this Contract. Payment may only be made after the delivery and acceptance of goods or services. The Vendor shall submit invoices in arrears.

3.13 Invoicing, Billing and Payment Methods

WV PEIA requires to be invoiced on a monthly or quarterly basis for administrative and all costs for the prior month(s). The preferred method of payment by the State of West Virginia is electronic funds transfer or Pcard (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

3.14 Additional Fees

Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. **Including such fees or charges as notes to the solicitation may result in rejection of the vendor's bid.** Requesting such fees or charges be paid after the contract has been awarded may result in **cancellation of the contract**. Other fees include but are not limited to **travel costs, penalties or interest.**

3.15 Taxes

The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

3.16 Funding

This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available.

3.17 Cancellation

The PEIA Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The PEIA Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules.

3.18 Time

Time is of the essence with regard to all matters of time and performance in this Contract.

3.19 Applicable Law

This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code or West Virginia Code of State Rules is void and of no effect.

3.20 Compliance with Laws

Vendor understands that any and/or all work performed under the scope of any contract award shall be performed in accordance and compliance with any and/or all applicable State and/or federal laws, rule(s) and/or regulation(s). This shall include full compliance with any State and/or Federal laws enacted during the term of the proposed Agreement or contract. Such compliance includes, but is not limited to, compliance with:

1. The Genetic Information Non-discrimination Act of 2008 (GINA) - (Pub.L. 110–233, 122 Stat. 881, enacted May 21, 2008)
2. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (PUBLIC LAW 104-191)
3. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009
4. The Privacy Act of 1974, as amended, 5 U.S.C. § 552a
5. The Consolidated Appropriations Act of 2021, otherwise known as the "No Surprises Act", (H.R. 133; Division BB – Private Health Insurance and Public Health Provisions).
6. NIST Guidance referenced in and as applicable to compliance with the above referenced law, e.g. NIST SP 800-53; NIST SP 800-66; NIST 800-88
7. The Patient Protection and Affordable Care Act (ACA) (''PPACA''; Public Law 111–148)
8. West Virginia Code §5-16-1, et seq.
9. West Virginia Code §33-51-3
10. West Virginia Code §33-51-4
11. West Virginia Code §33-51-7
12. West Virginia Code §33-51-8
13. West Virginia Code §33-51-9(c) & (d)
14. West Virginia Code §33-51-10
15. West Virginia Code §33-54-1, et seq.
16. West Virginia Code §33-15-4s(g)
17. West Virginia Code §33-24-7s(g)
18. West Virginia Code §33-25-8p(g)
19. West Virginia Code §33-25A-8s(g)
20. West Virginia Code §33-58-1
21. West Virginia Code §33-15B-1, et seq.
22. West Virginia Code §33-16E-1, et seq.
23. All applicable provisions of the Privacy and Security Rules of HIPAA found in 45 CFR Part 160 and Part 164, Subparts A and E, and 45 CFR Part 160 and Subparts A and C of Part 164.

By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

Subcontractor Compliance: Vendor shall notify all subcontractors providing commodities or services related to this Contract that, as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances.

3.21 Arbitration

Any references made to arbitration contained in this Contract and Vendor's bid are null and void.

3.22 Modifications

This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary, no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor.

3.23 Waiver

The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

3.24 Subsequent Forms

The terms and conditions contained in the signed executed contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained therein.

3.25 Assignment

Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency and any other government agency or office that may be required to approve such assignments.

3.26 Warranty

The Vendor expressly warrants that the goods and services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

3.27 State Employees

State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

3.28 Privacy, Security, and Confidentiality

The Vendor shall be deemed a Business Associate of the Agency as defined by HIPAA and shall be subject to the terms and conditions of the State of West Virginia Executive Branch Business Associate Agreement (WV BAA) and the State of West Virginia Executive Branch Data Management Addendum (WV DMA). The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information, protected health information either in identified or de-identified formats, or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements (CPISAR), set forth in

http://www.state.wv.us/admin/purchase/privacy/default.html

Vendor shall be responsible for ensuring that all subcontractors performing any of the scope of work related to this Agreement are informed of the terms and conditions of the WV BAA, the WV DMA, and the CPISAR and that such subcontractors agree to compliance with the same.

All information used, sent, stored, transmitted or otherwise maintained by the Vendor shall be stored in a NIST compliant secure format and shall be encrypted at rest and in transit. The Vendor shall apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. See 45 CFR 164.530(c).

All personally identifiable information (PII) and protected health information (PHI) shared or given to the Vendor by the Agency shall remain the property of the Agency with no ownership rights expressed or conveyed.

PEIA reserves the right to conduct certain "vendor assurance audits" to ensure the Vendor's compliance with the applicable provisions of HIPAA, HITECH, and any other laws, rules, and regulations that relate to the privacy, security, confidentiality, and integrity of the PII and PHI that may be created, used, managed, or transmitted under the Scope of Work of this Contract.

Within 90 days of the termination of the contract, the Vendor shall submit to Agency a HIPAA/NIST compliant Data Disposition plan that clearly defines and details how the PII/PHI used in this contract shall be rendered unreadable, unusable, or otherwise indecipherable in accordance with NIST SP 800-88.

The Vendor agrees that all member service call recordings and notes between the Vendor and PEIA members will be PEIA's property.

3.29 Licensing

In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and

requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

3.30 Subcontractor Compliance

PEIA requires Vendors to notify us and provide us a list of all subcontractors who may be performing any part of the scope of work on a project. PEIA reserves the right to approve all current and future subcontractors for this project and require the apparent successful bidder to replace subcontractors to all provisions of the contract. No subcontractor may perform work under this contract without express written consent of PEIA.

Vendor must be able to assume responsibility for all contractual activities offered in this proposal, whether or not that bidder directly performs them. Responsibility includes, but is not necessarily limited to: quality of work/service/products delivered; on-time delivery; staff conduct/behavior; accuracy of reports and billing; and representing PEIA in a professional manner as a vendor and service provider to our members. The vendor will be the sole point of contact with regard to contractual matters, including payment of any and all charges resulting from the anticipated contract.

Vendor shall notify all subcontractors providing commodities or services related to this Contract that, as subcontractors, they too are bound by all terms, conditions, and caveats of this RFP and are required to comply with all applicable laws, regulations, and ordinances as described in Section 3.20.

Vendor shall notify all subcontractors providing commodities or services related to this Contract that, as subcontractors, they too are required not to disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules as described in Section 3.28. Subcontractors must further agree to the terms and conditions of the WV BAA, the WV DMA, and the CPISAR as set forth in Section 3.28.

Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in Section 3.29.

In accordance with applicable provisions of 45 CFR § 164.512(e)(1)(i) and (f)(1)(ii), the Vendor is required to notify the Agency within five (5) business days if it or any of its subcontractors are involved or engaged in any litigation which may result in the disclosure or re-disclosure of any Agency member PII/PHI in an identified or de-identified format. The

State of West Virginia and the Agency reserve the right to defend against any such disclosures or re-disclosures.

3.32 Antitrust

In submitting a bid to, signing a contract with, or accepting an Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing or unreasonable restraint of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

3.33 Vendor Certifications

By signing its bid or entering into this Contract, Vendor certifies (1) that its bid or offer was made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership, person or entity submitting a bid or offer for the same material, supplies, equipment or services; (2) that its bid or offer is in all respects fair and without collusion or fraud; (3) that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; and (4) that it has reviewed this Solicitation in its entirety; understands the requirements, terms and conditions, and other information contained herein.

Vendor's signature on its bid or offer also affirms that neither it nor its representatives have any interest, nor shall acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency. The individual signing this bid or offer on behalf of Vendor certifies that he or she is authorized by the Vendor to execute this bid or offer or any documents related thereto on Vendor's behalf; that he or she is authorized to bind the Vendor in a contractual relationship; and that, to the best of his or her knowledge, the Vendor has properly registered with any State agency that may require registration.

3.34 Vendor Relationship

The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation

and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold the State and Agency harmless from, and shall provide the State and Agency with a defense against, any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

3.35 Indemnification

The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

3.36 Conflict Of Interest

Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

3.37 Reports

Vendor shall provide the Agency with the following reports identified by a checked box below:

[X] Such reports as the Agency may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

[X] Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency.

All reports should be delivered to the PEIA via email at peiadirector@wv.gov.

3.38 Background Check

In accordance with W. Va. Code § 15-2D-3, the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the buildings of PEIA or State of West Virginia or who have access to sensitive

or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository. The service provider is responsible for any costs associated with the fingerprint-based state and federal background inquiry. After the contract for such services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the PEIA or State of West Virginia or have access to sensitive or critical information, the service provider shall submit a list of all persons who will be physically present and working in the State of West Virginia buildings to the Director of the Division of Protective Services for purposes of verifying compliance with this provision. The State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check.

Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

3.39 Communications

From the time the RFP is released and until a successful Bidder is announced by WV PEIA, news releases pertaining to this document or the services, study, data, or project to which it relates, shall not be made without prior written WV PEIA approval, and then only in accordance with the explicit written instructions from WV PEIA. No results or presentations of the program, with or without mentioning WV PEIA are to be released without prior written approval of WV PEIA and then only to persons designated.

All communications pieces to be used as part of the program shall require written approval of PEIA prior to their distribution. The cost of said communications pieces should be included in the vendor pricing submitted.

3.40 Final Services and Programming

Vendors must agree that final services and programming options will be decided by PEIA in coordination with the winning vendor. The proposing company must begin implementation within thirty (30) calendar days of the awarding of the contract or an otherwise agreeable time frame.

3.41 Project Launch

At the discretion of the PEIA Director, a one-time $20,000 penalty may be assessed in the event that the program does not meet scheduled final testing or launch deadlines due to vendor fault.

3.42 Litigation Bond

Each Bidder responding to this RFP is required to submit a litigation bond in the amount of 5% of submitted bid based only on annual administrative fees, made payable to the West Virginia Public Employees Insurance Agency. In lieu of a litigation bond, bidder may submit a litigation waiver form. A surety company licensed to do business in the State of West Virginia with the West Virginia Insurance Commission, on a form acceptable to the State,

and countersigned by a West Virginia Resident Agent must issue this bond. The only acceptable alternate forms of the bond are (1) company certified check (not an individual) and (2) a cashier's check. The purpose of the litigation bond is to discourage unwarranted or frivolous lawsuits pertaining to the award of a contract from this RFP. Secondly, the bond provides a mechanism for the State of West Virginia, the Agency, and its officers, employees, or agents thereof to recover damages, including (but not limited to) attorney fees, loss of revenue, loss of grants or portions thereof, penalties imposed by the federal government and travel expenses which may result from any such litigation. A claim against the bond will be made if the Bidder contests the award in a court of competent jurisdiction and the grounds are found to be unwarranted or frivolous based on the facts of the award or applicable law as determined by the court.

The bond or alternate form must remain in effect for two years from the proposal submission date. After six (6) months, each Bidder may request, and the State anticipates granting, a release of the litigation bond or alternate form. However, the Bidder will be required to provide a release (signed and notarized in a form that is acceptable to the State) prior to release of the bond which states that the Bidder will not sue. Failure to submit an appropriate bond or Litigation Waiver Form with the proposal at the time of bid opening will result in automatic disqualification of the Bidder's proposal and the proposal will be considered non-responsive. The Litigation Waiver form would need to be completed and submitted with the proposal in place of a litigation bond. The Bidder would completely waive and forgo any and all legal right or ability the Bidder may now have, or in the future, to initiate any sort of challenge to or against the selection of a Bidder and/or the ultimate award of a contract pursuant to the RFP. Additional details are within the Litigation Waiver Form. See Attachment 9.

SECTION 4: AGENCY & PROJECT INFORMATION

4.1. Agency Background and Current Operating Environment:

PEIA is an agency of the State of West Virginia which administers benefits for approximately 74,101 active employees and COBRA participants. PEIA also administers benefits for 43,547 retired employees and surviving dependents on behalf of the West Virginia Retiree Health Benefits Trust Fund. There are 103,000 eligible dependents, resulting in approximately 216,000 members being covered by the PEIA health plan. Combined total annual premiums and capitations are approximately $1.2 billion for the fiscal year ending June 30, 2026.

A comprehensive fee-for-service health benefit plan, the Preferred Provider Benefit (PPB) plan, is offered to all eligible participants statewide (as well as members in other jurisdictions) and is administered by a Third Party Administrator (TPA) (medical claims are administered by UMR) and a Pharmacy Benefits Manager (PBM) (pharmacy claims are administered by Express Scripts aka ESI). PEIA also offers a managed care plan option statewide, and currently contracts with a managed care organization, The Health Plan.

In the PEIA PPB Plans and the Prescription Drug plan, participants are responsible for cost sharing in the form of an annual deductible, coinsurance, and copayments. Amounts paid by the individual apply to a separate annual prescription deductible and out-of-pocket amount and do not apply to the annual deductible and maximum medical out-of-pocket amount, except for the PPB Gold High Deductible Plan and the PPB WV Bronze High Deductible Plan (approximately 13,500 members total), which have a combined medical and prescription drug deductible and out-of-pocket.

Participants in the PPB Plan may use any provider in West Virginia they choose; they are not required to use a select group of providers, nor must they go through primary care providers to gain access to more specialized providers. By law, all providers in West Virginia who provide health care services or supplies to PEIA members must accept assignment of benefits and cannot bill PEIA patients for any amount by which their charges exceed the maximum fees established by PEIA for each service.

PEIA employs a variety of techniques for the PPB plan that are characteristic of managed care programs:

- utilization review, consisting of prior approval for specific procedures and/or out-of-network care, precertification of hospital inpatient admissions and certain outpatient procedures, case management of high utilizer and/or high dollar cases, disease management for chronic conditions and care coordination through a predictive modeling program;
- a provider fee schedule employing the Resource-Based Relative Value Scale (RBRVS) which represents a discount from most providers' usual charges, and which is enforced by statute prohibiting in-state providers from billing PEIA insureds for charges other than applicable copays, coinsurance, deductibles, and non-covered services;
- an outpatient prescription drug plan that utilizes a nationwide network of participating providers throughout the state and elsewhere which have agreed to discount prices, and which submit claims electronically to a separate third-party administrator (ESI);
- a contracted network of hospitals and professional providers, both inside and outside the state, that perform organ transplant services for pre-negotiated rates;
- a contracted network of hospitals and professional providers, nationally, for members who must obtain services outside West Virginia;
- pre and post payment reviews by its TPA, including but not limited to DRG validation, and the Claim Edit System (CES); The CES is published by OptumInsight which is part of Optum, Inc. The CES system is designed to analyze professional claims. The CES system will look at the data on each claim and check for errors, omissions, and questionable coding relationships.
- a prospective payment system (PPS) for inpatient hospital reimbursement; and

- an ambulatory payment classification system (APC) for outpatient hospital reimbursement.

Benefits, premiums, and cost-sharing mechanisms are set annually by the PEIA Finance Board and are based upon the plan actuary's projected financial results with given consideration to anticipated utilization and enrollment.

Open enrollment is held each spring for plan selection. The fiscal year under which the State allocates funding is July 1 through June 30, which is also the PEIA benefit plan year. (Note: If a member becomes Medicare primary mid-year, they will move to the Special Medicare plan and will remain there until December 31. On January 1, the Special Medicare Plan members are moved to Humana. A very small percentage of Special Medicare Plan members stay in the Special Medicare Plan with UMR and Express Scripts rather than switching to Humana on January 1). The PEIA reserves the right to implement any changes affecting benefits and premium contribution within the plan, as deemed appropriate, or as mandated by legislative action.

State, higher education, and some public-school employees participating in PEIA have the ability to pay medical and life premiums on a pretax basis through a premium conversion plan, which is an IRS approved Section 125 plan.

Employees and retirees may elect to participate in Mountaineer Flexible Benefits which offers coverage for vision, dental, long- and short-term disability, and medical and dependent care spending accounts. These optional benefits are funded wholly by participating employees and are administered by a separate third-party vendor, currently FBMC. Premiums for these optional benefits are paid on a pre-tax basis through a Section 125 Plan.

PEIA has a Comprehensive Care Partnership (CCP) Program that is designed to allow members to take more responsibility for their primary care and focuses on preventive care as opposed to reactive care. Members receive reduced or waived copayments for participating in the CCP.

For more information regarding PEIA, potential Bidders may research our website at **www.peia.wv.gov**.

4.2. Project Description: PEIA is seeking to obtain a qualified vendor to perform post payment claim review services on PEIA's behalf such as recognizing and flagging member eligibility and provider billing abnormalities indicative of fraud, waste, or abuse; identifying, investigating and recovering overpayments; collaborating with PEIA's Third Party Administrator (TPA) to implement prepayment reviews of claims submitted by providers identified as outliers to prevent improper payments; and collaborating with the Agency's Pharmacy Benefit Manager (PBM) to implement post-payment processes to reduce and recover improper payments more effectively and efficiently. Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches.

Vendor must be able to assume responsibility for all contractual activities offered in this proposal, whether or not that bidder directly performs them. Responsibility includes but is not necessarily limited to: quality of work/service/products delivered; on-time delivery; staff conduct/behavior; accuracy of reports and billing; and representing PEIA in a professional manner as a vendor. The vendor will be the sole point of contact with regard to contractual matters, including payment of any and all charges resulting from the anticipated contract.

It shall be the responsibility of the vendor to prepare, in a clear and concise manner, a compelling submission that fulfills the intent and scope of this solicitation.

4.3. Project Goals and Objectives – The project goals and objectives are listed below.

4.3.1. To increase the amount of money recovered by PEIA through administrative actions, civil settlements, and criminal recoveries resulting from the vendor's efforts to identify and investigate instances of fraud, waste or abuse in PEIA's operations.

4.3.2. To obtain a favorable ROI whereby the amount of money PEIA spends on the vendor's services is exceeded by the amount of money PEIA saves and recovers in healthcare expenditures resulting from the vendor's services.

4.3.3. To improve public awareness of PEIA's efforts to protect the financial integrity and stability of its Plans by reducing FWA in its operations and recovering overpayments.

SECTION 5: MANDATORY REQUIREMENTS

The following mandatory requirements must be met by the Vendor as a part of its submitted proposal. Vendors should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. The terms "must", "will", "shall", "minimum", "maximum", or "is/are required" identify a mandatory item or factor. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. Decisions regarding compliance with any mandatory requirements shall be at the sole discretion of PEIA. The vendor must include an affirmation in their response that they agree to and will comply with the mandatory requirements listed below on Attachment 3 (Mandatory Requirements Confirmation).

5.1 Minimum Project Requirements

5.1.1 Vendor agrees and understands that it will be performing an Administrative service and/or function on behalf of PEIA and is therefore a "Business Associate" of PEIA as defined by 45 CFR § 160.103 and agrees to sign the State of West Virginia

Executive Branch Business Associate Agreement in accordance with the applicable provisions of 45 C.F.R. § 164.502(e) and § 164.504(e).

5.1.2 Vendor's project plan must include an implementation timeline.

5.1.3 Vendor will evaluate PEIA's medical and pharmaceutical claims data based on plan designs, West Virginia and federal laws, regulations and policies, Centers for Medicare & Medicaid Services (CMS) standards, and other applicable requirements to determine if claims were processed and paid correctly as submitted.

5.1.4 Vendor will analyze PEIA's claims data to identify the provider(s) or provider types, services, or claims types that should be subject to further review in detecting FWA.

5.1.5 Vendor will identify aberrant provider billing patterns and behavior using peer comparison, data mining, rules-based, artificial intelligence (AI) and/or other analytics.

5.1.6 Vendor will field, triage, and evaluate complaints and referrals related to FWA in PEIA's operations received via telephone, hotline, email, fax, web portal, or any other means.

5.1.7 Vendor will prioritize and recommend which procedure types or categories, provider types, individuals and/or entities should be the focus of FWA investigations.

5.1.8 Vendor will request, obtain, evaluate, and audit medical records, employee files, time sheets and other relevant documents to determine whether providers submitted claims appropriately and/or whether individuals enrolled in PEIA's plans were eligible for enrollment, using a secure, web-based portal that allows healthcare providers and others to electronically upload digital copies of medical records and other responsive documents.

5.1.9 Vendor will evaluate and audit claims on an itemized, line-by-line basis as they were adjudicated or as they should have been adjudicated after reviewing medical records and other relevant documents for coding accuracy, clinical documentation alignment, and compliance with applicable policies and documentation requirements.

5.1.10 Vendor will plan and conduct sensitive and complex investigations into suspected FWA, including but not limited to record reviews, claims data analysis, interviews, interrogations, evidence collection, surveillance, and database research.

5.1.11 Vendor will participate in joint investigations with West Virginia and federal agencies that investigate, litigate, and/or prosecute healthcare FWA allegations.

5.1.12 Vendor will communicate detailed audit and investigation findings to the PEIA Director to identify ineligible members and aberrant providers via print, electronic, telephonic and virtual means.

5.1.13 Vendor will present the PEIA Director with options for recovery of overpayments, corrective action recommendations for providers, and PEIA operational improvement recommendations identified through its FWA investigations.

5.1.14 Vendor will initiate and participate in FWA overpayment recovery actions on a case-by-case basis as directed by the PEIA Director, ensuring that all staff members who participated in an investigation are available to execute affidavits, attend depositions, and offer sworn testimony at depositions or in courtroom proceedings in support of PEIA's claims.

5.1.15 Vendor will provide, manage, and update a secure case file management system with capability to store case notes and documents (medical records, employee records, correspondence, Personal Health Information (PHI), etc.) which must contain an easy to use Graphical User Interface (GUI) providing designated PEIA personnel with full access to all case materials, a dashboard reflecting relevant performance measures, and the ability to create ad-hoc reports and generate reports based on any data captured in the system.

5.1.16 Vendor will provide PEIA with additional customized and detailed reports upon request no later than five (5) business days after receiving the request.

5.1.17 Vendor will possess a robust roster of trained coding, auditing, nursing, documentation, compliance, and investigative personnel with demonstrated experience conducting healthcare audits and healthcare fraud investigations.

5.1.18 Vendor will ensure that all staff members assigned to work on PEIA's cases possess sufficient knowledge, experience, expertise, and training to successfully complete their assigned tasks and duties.

5.1.19 Vendor will ensure compliance with and responsiveness to required PEIA vendor auditing processing, including but not limited to vetting assigned personnel through the OIG List of Excluded Individuals/Entities (LEIE) and the System for Award Management (SAM or sam.gov).

5.1.20 Vendor will participate in regular meetings on at least a monthly basis with designated PEIA staff members to discuss cases and performance measures, answer questions, and ensure the Agency is fully informed of the Vendor's activities.

5.1.21 Personnel assigned by Vendor to work on PEIA's cases will participate in regular meetings with other State and federal government agencies such as the West

Virginia Office of the Insurance Commissioner (OIC), the West Virginia Medicaid Fraud Control Unit (MFCU), United States Attorney's Offices, and County Prosecuting Attorneys upon request and as needed to protect PEIA's financial interests and ensure accountability for criminal violations by PEIA members, providers, and/or contractors.

5.1.22 Vendor will perform statistically valid random sampling (SVRS) and mathematical extrapolation of overpayments across a provider's wider billing universe based on SVRS findings.

a. *Standards:* Any SVRS and extrapolation methodology executed by the Vendor must strictly adhere to recognized federal standards, specifically utilizing the U.S. Department of Health and Human Services Office of Inspector General (HHS-OIG) RAT-STATS software or an equivalent, mathematically validated methodology.

b. *Application:* The line-by-line findings from the audited sample shall form the legal and mathematical baseline for projecting the total overpayment amount.

c. *Discretion:* The choice between a 100% line-by-line universe audit and an SVRS extrapolated audit shall be determined on a case-by-case basis, subject to the final review and written approval of the PEIA Director.

5.1.23 Vendor must confirm and agree that any and/or all data received from PEIA and/or used by the Vendor shall be kept secure in accordance with applicable provisions of the HIPAA Security Rule(s) and applicable NIST Standards and/or Guidance including, but not limited to, appropriate security and encryption when being transmitted and when at rest.

5.1.24 Vendor must guarantee a minimum Return On Investment (ROI) from its services no less than 2:1. The methodology to determine ROI must be clear and well defined.

5.1.25 Vendor must agree that all data collected, created, shared, or generated under the scope of work of this contract will be kept secured, encrypted, and segregated in a manner so that, if needed and/or upon termination of the contract it can be rendered unreadable, unusable or indecipherable or otherwise destroyed in accordance with applicable provisions of the HIPAA Security Rules. The referenced data is the sole property of the West Virginia Public Employees Insurance Agency (PEIA) and may not be used for any other projects, contracts, or purposes without the express written consent of PEIA. Any severance or change in status of a subcontractor, employee, collaborator, student, or agent, whether voluntary or involuntary, shall immediately terminate their rights to access, use, or otherwise have direct or indirect permissions with regard to said data. Under no circumstances will any PEIA data, neither in an identified form nor in a deidentified format, be stored, transmitted/sent, used, or otherwise viewed outside the Continental United States. PEIA data may only be used for the fulfillment of the scope of work under the proposed contract or Agreement and may not be used for any other purpose.

5.1.26 The vendor must utilize systems/software that support a secure data management structure that is compliant with any and/or all State and/or federal security and privacy laws, rules, regulations, and/or standards.

5.1.27 Vendor agrees and understands that any contract or award made under this solicitation shall be governed by the laws of the State of West Virginia.

5.2 Minimum Vendor Requirements

5.2.1 Vendor shall provide information and documentation in **Attachment 14 (Staff Resumes)** regarding the firm's staff qualifications and experience in performing post payment medical and pharmaceutical claim review services and conducting healthcare FWA investigations as described in Section 4.2 above.

Proposal staffing must include at least one (1) Investigations Manager with at least five (5) years of experience managing healthcare FWA investigations that will be available to address PEIA's cases, needs, and issues on a daily basis. This Investigations Manager should have successfully led at least one other major account through implementation and project management. This individual shall be present on this account for both implementation and ongoing management.

Information and documentation shall include, but is not limited to:

- Copies of any staff certifications or degrees to demonstrate the qualifications of leadership, project management, expertise in performing post payment claim review services such as recognizing and flagging member eligibility and provider billing abnormalities indicative of FWA through data mining or other techniques and conducting complex healthcare fraud investigations.
- Proposed staffing plans for a Special Investigations Unit serving a health plan the size of PEIA in terms of both covered lives and total healthcare expenditures.
- Descriptions of past projects completed (descriptions shall include the location of the project; project manager's name and contact information; type of project; the project goals and objectives; and how they were met.)
- Any other information that the vendor deems relevant to the items identified as desirable or mandatory below.

5.2.2 Vendor shall submit a company summary including company history, office location(s), company size, financial summary from most recent fiscal year (including total revenue, total liabilities, total assets, and net margin not to exceed four (4) pages), and statement of technical areas of expertise. The Vendor must be

able to substantiate that the Vendor has sufficient resources to complete the project successfully within the time requirements.

5.2.3 Vendor shall provide at least 3 active client references and 3 terminated client references in **Attachment 13 - Vendor Experience Form.** Vendor may substitute additional active client references for the 3 terminated client references, but Vendor must submit at least 6 total client references.

5.2.4 Vendor shall provide the following **Financials and Ratings** information:

- Certificate of Insurance
- Financial statements
- Accreditations, if any
- Financial ratings, if any

5.2.5 Vendor will provide a list of any current subcontractors, collaborators, and other third parties that will perform duties under this contract, including firm name and address, contact person, complete description of work to be subcontracted, and descriptive information concerning subcontractor's organizational abilities. This information will be provided with the bid proposal in **Attachment 12 (Subcontractor Information Form)**.

5.2.6 Vendor must demonstrate a minimum of four (4) years of experience conducting complex healthcare FWA investigations as evidenced by contracts in place for at least five (5) years, at least two (2) years of which include conducting complex healthcare fraud investigations for a health plan client with at least 50,000 covered lives.

5.2.7 Vendor shall provide information and demonstrate that it has experience conducting complex healthcare FWA investigations involving providers in rural areas. Vendor may demonstrate this experience by listing clients as a reference or providing evidence of such investigations that Vendor successfully completed including the results obtained from such investigations.

5.2.8 Vendor must be, and must remain, compliant with all federal regulations impacting healthcare fraud investigations, including but not limited to compliance with HIPAA and all related privacy and security regulations.

5.2.9 Vendor must agree to immediately (no more than one (1) business day) report any event or incident that may result in any real or perceived harm to any member, provider, or the Agency.

5.2.10 The vendor shall agree in accordance with applicable provisions of 45 CFR § 164.512(e)(1)(i) and (f)(1)(ii), the vendor, or any subcontractor of the vendor, is required to notify PEIA within five (5) business days if it is involved or engaged in any litigation which can or may result in the disclosure or re-disclosure of any PEIA

member PII/PHI in an identified or de-identified format. The State of West Virginia and PEIA reserve the right to defend against any such disclosures or re-disclosures.

5.2.11 Vendor must have at least one (1) staff member assigned to work on PEIA's cases who is a full-time resident of West Virginia and possesses at least three (3) years of professional experience working on healthcare FWA investigations and possesses a valid West Virginia drivers license.

5.2.12 Vendor must have demonstrated experience coordinating with a commercial or public sector health plan's TPA, PBM, and data warehouse vendor to obtain access to claims data in a secure manner that complies with any and/or all State and/or federal security and privacy laws, rules, regulations, and/or standards.

5.2.13 Vendor shall identify any projects within the last ten (10) years where the Contract in question was cancelled, terminated for cause, or any litigation related to Vendor's past performance was initiated.

5.2.14 Vendor shall supply an attestation (written documentation) of a favorable background check, at the expense of the Vendor for Vendor personnel who might reasonably be expected to access sensitive and confidential client data contained in any system accessed during the Contract. The Agency may request the removal of staff for disqualifying offenses.

5.3 Minimum Performance Guarantee

It is PEIA's intention and expectation that the savings achieved through this solicitation shall more than cover the costs of the Vendor's services. As described in Section 5.1.24 above, the Vendor must guarantee a minimum Return On Investment (ROI) from its services no less than 2:1. The methodology to determine ROI must be clear and well defined.

SECTION 6: TECHNICAL RESPONSE QUESTIONS

The following detailed questions correspond to the mandatory requirements for the Vendor and must be answered fully in the technical proposal. **Failure to provide adequate information will result in reduced technical scores.**

6.1 Technical Response Questions

6.1.1 Please describe your company's experience working with state government clients and/or government clients

6.1.2 Please describe the account team's experience working with commercial health plans that are similar to the client.

6.1.3 Confirm that the client will have direct or dedicated account team support for continuity of knowledge and history to expedite and support its needs.

6.1.4 Confirm what version of the TLS (Transport Layer Security) line your organization uses for secure communication with your clients.

6.1.5 How many times will the account team meet with the client in person during the year?

6.1.6 Please confirm that, at a minimum, bi-annual and annual performance reviews will be conducted by the account team for the client.

6.1.7 Please confirm the account team will be involved in the implementation process.

6.1.8 What is the turnover rate of your Account Managers?

6.1.9 Please confirm you will provide 30-day notice of an account team change (other than in the case of employee resignation/termination).

6.1.10 Please confirm that a specific, dedicated team will be assigned to the client for the duration of the client's implementation.

6.1.11 Describe the implementation process, including required tasks for the client's team.

6.1.12 Please confirm that you will send detailed activity reports to the client on a bi-weekly basis.

6.1.13 Please confirm that you will send administrative invoices to the client on a monthly basis.

6.1.14 Please confirm you have reviewed the West Virginia state invoicing requirements shown as Attachment 5.

6.1.15 Confirm you will waive any charges to PEIA or PEIA's vendors such as data feed set-up, or programming fees for establishing a connection with the PBM, data warehouse, TPA, or other external vendor for real-time, bidirectional data integration, including nonstandard data integration formats. **Currently PEIA utilizes a flat file for the TPA, data warehouse, an external vendor, and an Access file database and/or Excel for PEIA and expects to continue using these formats.**

6.1.16 Describe your reporting capabilities, including weekly, monthly, quarterly, and annual reports, as well as online reporting access. Please provide sample reports.

6.1.17 Please provide the annual dollars at risk being offered to the client as Performance Guarantees.

6.1.18 Please outline the amount, terms, allocations, and details for your Performance Guarantee offer.

6.1.19 Please confirm that you are willing to offer separate implementation guarantees.

6.1.20 Please outline any additional Performance Guarantees you are offering.

6.1.21 Please confirm that you are willing to customize Performance Guarantees based on the client's business objectives.

6.1.22 Provide an itemized list of all your revenue sources.

6.1.23 Are you prepared to put 100% of your administrative fees at risk if the total net savings generated from your service do not exceed the total expenditures and fees for your service?

6.1.24 Describe your process for refunding PEIA if the guarantee is not met.

6.1.25 What is your proposed minimum guaranteed savings-to-fee ratio (e.g., 2:1 or 3:1)?

6.1.26 Does your guarantee cover only the 'break-even' point, or do you guarantee a specific ROI above your costs?

6.1.27 Describe your methodology for determining savings and ROI. For the purposes of calculating the ROI, savings shall be strictly limited to:

Hard Recoveries: Actual overpayment dollars recovered, collected, and deposited back into PEIA accounts resulting from the Vendor's post-payment audits.

Explicit Exclusions (Soft Savings): The Vendor shall not include hypothetical savings, projected future behavioral changes by providers, estimated legal fees avoided, or any uncollected "identified" overpayments that are overturned on appeal or deemed uncollectible.

SECTION 7: VENDOR PROPOSAL

Proposal Submission Information: All bids must be received by the Agency by the due date. Any bid received by PEIA is considered to be in the possession of the Agency and will not be returned for any reason. Bids should be prepared as follows:

7.1 **Economy of Preparation:** Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

7.2 Vendor must restate all questions and all pages should be sequentially numbered. Responses to this solicitation should not exceed seventy-five (75) pages.

7.3 **Incurring Cost:** Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

7.4 **Two-Part Submission:** Vendors must submit two distinct proposals: a Technical Proposal and a Cost Proposal. Technical proposals must not contain any cost information relating to the project. If Vendor submits a litigation bond instead of a litigation waiver, the litigation bond must be included in the Cost Proposal and the Technical Proposal should *only* clearly confirm that a litigation bond is provided without including monetary details of the bond.

> **Required:** One (1) searchable electronic copy of EACH proposal. Cost and Technical proposals must be prepared as separate documents and submitted separately: as separate, clearly marked electronic files; as separate, clearly marked digital media; or as separate, clearly marked emails.

7.5 **Title Page:** State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.

7.6 **Response Reference:** Vendor's response should clearly reference how the information provided applies to the RFP request to ensure that PEIA can easily find information and determine how it relates to all mandatory requirements and requested information.

7.7 **Bid Details:** Bids should contain the information listed below in the body of each email or on the face of each physical proposal.

SEALED BID: Special Investigations Unit (SIU) Services
SOLICITATION NO: ARFP PEI2700000001

VENDOR NAME: *Vendor Name, Address and Telephone Number*
CONTACT: *Primary Vendor Contact Name and Email Address*
PROPOSAL TYPE: *Technical Proposal or Cost Proposal*

7.8 **Legal Basis:** The procurement process for this RFP will be conducted in accordance with the procurement policies and procedures established by PEIA in the Plan Document (151

CSR 01). This procurement is exempt from some requirements of the West Virginia Purchasing Division pursuant to W. Va. Code §5A-3-10b.

7.9 Proposal Withdrawal: Prior to the proposal due date, a Vendor may withdraw their proposal by submitting a written request signed by the Vendor's authorized agent. The written withdrawal request will be directed to the PEIA Procurement Officer. A valid justification for the request must be provided and PEIA will determine whether or not to allow the withdrawal.

7.10 Oral Presentations: At the option of PEIA, oral presentations by selected Vendors may be required. Vendors will be notified if an oral presentation is required. The Vendors should present complete, comprehensive proposals without relying on oral presentations, because PEIA reserves the right to award a contract without further discussions or an oral presentation. The Vendors may be requested to provide demonstrations of their proposed systems as part of their presentations. Presentations will be recorded, and any representations made during the oral presentation will become part of the Vendor's proposal and are binding if a contract is awarded.

7.11 Site Visits: PEIA may request a site visit to review the Bidder's facilities or its subcontractors' facilities. This may include, but not be limited to, a review of policies and procedures, and any other area of operation that directly or indirectly affects the provisions of the RFP, Contract or the delivery of health care services.

Any cost incidental to the site visit by the Bidder shall be borne by the Bidder. PEIA will be responsible for its own travel and accommodations.

A readiness review may also be conducted on-site at the selected Bidder's facilities following execution of the Contract and before implementation of the Special Investigations Unit services.

7.12 Protest of Intended Award: Vendors that submit a litigation bond may protest an award in accordance with the procedure detailed in the PEIA Procurement Policy (151 CSR 01).

7.13 Restrictions on communications with State and Other Personnel: From the issue date of this RFP until a successful Vendor is selected and announced, Vendors are prohibited from communicating with any PEIA staff about this procurement and restricting communication to the contacts listed in this document. This provision is not intended to restrict current Contractors from communicating with PEIA staff regarding ongoing operational matters. The only exceptions to this restriction may occur at the Bidder's conference, oral presentations, or site visits.

Lobbying with or otherwise contacting any PEIA staff about this solicitation outside of the established communication process will result in disqualification.

SECTION 8: EVALUATION AND AWARD

8.1 Evaluation Process: Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.

PEIA, at its option, may elect to conduct interviews and oral presentations with the top-rated bidders. There are no points specifically assigned to the interview. The purpose is to confirm or clarify responses to the RFP.

8.2 Evaluation Criteria: Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 60 of the 100 points. Cost represents 40 of the 100 total points.

8.3 Evaluation Point Allocation

All points awarded for each proposal component will be summed up to obtain a total figure. The Vendor who meets all the mandatory specifications and attains the highest point score of all Vendors shall be awarded the contract. The successful Vendor will be made by a consensus of the evaluation committee.

8.4 Technical Bid Opening: At the technical bid opening, the Agency will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.

8.5 Technical Evaluation: The Agency evaluation committee will review the technical proposals and assign points where appropriate.

8.6 Proposal Disqualification:

8.6.1 Minimum Acceptable Score ("MAS"): Vendors must score a minimum of 70% (42 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.

8.6.2 Failure to Meet Mandatory Requirements: Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.

8.7 Cost Evaluation: The Agency evaluation committee will review the cost proposals and assign points in accordance with the cost evaluation formula contained herein.

8.7.1 Cost Evaluation Formula: Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to

generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1: Lowest Cost of All Proposals / Cost of Proposal Being Evaluated = Cost Score Percentage

Step 2: Cost Score Percentage X Points Allocated to Cost Proposal = **Total Cost Score**

Example:

Proposal 1 Cost is $1,000,000

Proposal 2 Cost is $1,100,000

Points Allocated to Cost Proposal is 40

Proposal 1: Step 1 – $1,000,000 / $1,000,000 = Cost Score Percentage of 1 (100%)
Step 2 – 1 X 40 = Total Cost Score of 40

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091 (90.9091%)
Step 2 – 0.909091 X 40 = Total Cost Score of 36.36364

SECTION 9: VENDOR ATTACHMENTS TO INCLUDE WITH BID

(Please provide in unlocked format)

VENDOR ATTACHMENTS TO INCLUDE WITH BID		
REQUESTED ATTACHMENTS	**FORM NAME**	**CONFIRM INCLUDED**
1	Title Page	
2	Introduction	
3	Table of Contents	
4	Vendor Attachments to Include with Bid (Section 9)	
5	Certification and Signature Page, Signed (Section 11)	
6	Technical Response Questions	
7	Attachment 1: Intent to Bid Form	
8	Attachment 2: Cost Proposal (Pricing Page) **(submitted under separate cover from the Technical Proposal)**	
9	Attachment 3: Mandatory Requirements Confirmation	
10	Attachment 6: WV-96 Form	
11	Attachment 7: WV Data Management Addendum& Appendix	
12	Attachment 8: State of WV Executive Branch BAA (HIPAA Business Associate Addendum) & Appendix A	
13	Attachment 9: Litigation Waiver Form (or Litigation Bond with Cost Proposal)	
14	Attachment 10: WV Redaction Attestation Form	
15	Attachment 12: Subcontractor Information Form	
16	Attachment 13: Vendor Experience Form	
17	Attachment 14: Staff Resumes	
18	Attachment 15: Deviations Page	
19	Attachment 16: Addendum Acknowledgement Form	
20	Executive Summary that describes how your organization can best serve the client	
21	Template contract with proposal specific pricing and contract provisions	
22	Organizational Chart of the team that will be assigned to the client	
23	Customized implementation plan based on the timeline of the successful Vendor launching operations no later than January 1, 2027	

24	Sample Client Reports	
25	Performance Guarantees	
26	Description of data exchange process and formats (e.g. flat file, MS Access, Excel) for claims and eligibility feeds	
27	Detailed description of the Special Investigation Unit's proposed operations, including your proven ROI History	
28	Financials and Ratings Information (Section 5.2.4)	

SECTION 10: RFP ATTACHEMNTS

RFP ATTACHMENTS		
WV REQUIRED FORMS	**FORM NAME**	**VENDOR REQUIRED TO SUBMIT WITH PROPOSAL**
Attachment 1	Intent to Bid Form	YES
Attachment 2	Cost Proposal (Pricing Page)	YES
Attachment 3	Mandatory Requirements Confirmation	YES
Attachment 4	Vendor Registration Information	NO
Attachment 5	WV State Invoicing Requirements	NO
Attachment 6	WV-96 Form	YES
Attachment 7	WV Data Management Addendum & Appendix A	YES
Attachment 8	State of WV Executive Branch BAA (HIPAA Business Associate Addendum) & Appendix A	YES
Attachment 9	WV Litigation Waiver Form	YES (unless submitting a Litigation Bond with Cost Proposal
Attachment 10	WV Redaction Attestation Form	YES
Attachment 11	PEIA Master Services Agreement (MSA)	NO
Attachment 12	Subcontractor Information Form	YES
Attachment 13	Vendor Experience Form	YES
Attachment 14	Staff Resumes	YES
Attachment 15	Deviations Page	YES
Attachment 16	Addendum Acknowledgement Form	YES
Attachment 17	Addendum Detail	NO

SECTION 11: VENDOR SIGNATURE AND CERTIFICATION

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

_____
(Company)

_____
(Representative Name, Title)

_____
(Contact Phone/Email Address)

_____
(Date)

Attachment 1
Intent to Bid Form

Firms interested in submitting a proposal must return this "intent to Bid" to receive Data via secure FTP login

To:	WV Public Employees Insurance Agency RE: Special Investigations Unit (SIU) Services 601 57th Street SE, Suite 2 Charleston, WV 25304 Samuel.H.Revercomb@wv.gov

From:	**FIRM**		
	MAILING ADDRESS		
	CITY	**STATE**	**ZIP**
	NAME AND TITLE OF INDIVIDUAL		
	TELEPHONE NUMBER		
	FAX NUMBER		

Please consider this our intent to submit a proposal to the RFP issued by the Public Employees Insurance Agency of the Department of Administration for ARFP PEI2700000001, Special Investigation Unit (SIU) services.

SIGNED	**DATE**

Attachment 2

Cost Proposal (Pricing Page)

West Virginia Public Employees Insurance Agency

RFP Release date: **September 25, 2026**
RFP Due Date: **November 13, 2026**
Contract Effective Date: **January 1, 2027**

AMINISTRATIVE FEES	Year 1	Year 2	Year 3
All Inclusive Fixed Fee or All Inclusive PMPM Admin Fee	1/01/2027 - 12/31/2027	1/01/2028 - 12/31/2028	1/01/2029 - 12/31/2029
	$	$	$

COST PROPOSAL MUST BE SUBMITTED UNDER SEPARATE COVER FROM THE TECHNICAL PROPOSAL, I.E. SEPARATE ENVELOPE OR EMAIL CLEARLY MARKED

Attachment 3

Mandatory Requirements Confirmations

MANDATORY - THIS APPENDIX MUST BE COMPLETED AND INCLUDED WITH TECHNICAL PROPOSAL. VENDOR MUST MARK EACH ITEM TO INDICATE THAT THEY MEET THE CRITERIA OF OR AGREE TO THE SPECIFICATIONS OF EACH REQUIREMENT.

5.1 MINIMUM PROJECT REQUIREMENTS			
SECTION	**REQUIREMENT**	**CONFIRM/ DO NOT CONFIRM**	**ADDITIONAL INFORMATION IF DEVIATING**
5.1.1	Confirm that the Vendor agrees and understands that it will be performing an Administrative function on behalf of PEIA and is therefore a "Business Associate" as defined by 45 CFR § 160.103 and agrees to sign the State of West Virginia Executive Branch Business Associate Agreement in accordance with the applicable provisions of 45 C.F.R. § 164.502(e) and § 164.504(e).		
5.1.2	Confirm that Vendor's project plan will include an implementation timeline.		
5.1.3	Confirm that Vendor will evaluate PEIA's medical and pharmaceutical claims data based on plan designs, West Virginia and federal laws, regulations and policies, Centers for Medicare & Medicaid Services (CMS) standards, and other applicable requirements to determine if claims were processed and paid correctly as submitted.		
5.1.4	Confirm that Vendor will analyze PEIA's claims data to identify the provider(s) or provider types, services, or claims types that should be subject to further review in detecting FWA.		
5.1.5	Confirm that Vendor will identify aberrant provider billing patterns and behavior using peer comparison, data mining, rules-based, artificial intelligence (AI) and/or other analytics.		
5.1.6	Confirm that Vendor will field, triage, and evaluate complaints and referrals related to FWA in PEIA's operations received via telephone, hotline, email, fax, web portal, or any other means.		
5.1.7	Confirm that Vendor will prioritize and recommend which procedure types or categories, provider types, individuals and/or entities should be the focus of FWA investigations.		

5.1.8	Vendor will request, obtain, evaluate, and audit medical records, employee files, time sheets and other relevant documents to determine whether providers submitted claims appropriately and/or whether individuals enrolled in PEIA's plans were eligible for enrollment, using a secure, web-based portal that allows healthcare providers and others to electronically upload digital copies of medical records and other responsive documents.		
5.1.9	Vendor will evaluate and audit claims on a line-by-line basis as they were adjudicated or as they should have been adjudicated after reviewing medical records and other relevant documents for coding accuracy, clinical documentation alignment, and compliance with applicable policies and documentation requirements.		
5.1.10	Vendor will plan and conduct sensitive and complex investigations into suspected FWA, including but not limited to record reviews, claims data analysis, interviews, interrogations, evidence collection, surveillance, and database research.		
5.1.11	Vendor will participate in joint investigations with West Virginia and federal agencies that investigate, litigate, and/or prosecute healthcare FWA allegations.		
5.1.12	Vendor will communicate detailed audit and investigation findings to the PEIA Director to identify ineligible members and aberrant providers via print, electronic, telephonic and virtual means.		
5.1.13	Vendor will present the PEIA Director with options for recovery of overpayments, corrective action recommendations for providers, and PEIA operational improvement recommendations identified through its FWA investigations.		
5.1.14	Vendor will initiate and participate in FWA overpayment recovery actions on a case-by-case basis as directed by the PEIA Director, ensuring that all staff members who participated in an investigation are available to execute affidavits, attend depositions, and offer sworn testimony at depositions or in courtroom proceedings in support of PEIA's claims.		

5.1.15	Vendor will provide, manage, and update a secure case file management system with capability to store case notes and documents (medical records, employee records, correspondence, Personal Health Information (PHI), etc.) which must contain an easy to use Graphical User Interface (GUI) providing designated PEIA personnel with full access to all case materials, a dashboard reflecting relevant performance measures, and the ability to create ad-hoc reports and generate reports based on any data captured in the system.		
5.1.16	Vendor will provide PEIA with additional customized and detailed reports upon request no later than five (5) business days after receiving the request.		
5.1.17	Vendor will possess a robust roster of trained coding, auditing, nursing, documentation, compliance, and investigative personnel with demonstrated experience conducting healthcare audits and healthcare fraud investigations.		
5.1.18	Vendor will ensure that all staff members assigned to work on PEIA's cases possess sufficient knowledge, experience, expertise, and training to successfully complete their assigned tasks and duties.		
5.1.19	Vendor will ensure compliance with and responsiveness to required PEIA vendor auditing processing, including but not limited to vetting assigned personnel through the OIG List of Excluded Individuals/Entities (LEIE) and the System for Award Management (SAM or sam.gov).		
5.1.20	Vendor will participate in regular meetings on at least a monthly basis with designated PEIA staff members to discuss cases and performance measures, answer questions, and ensure the Agency is fully informed of the Vendor's activities.		
5.1.21	Personnel assigned by Vendor to work on PEIA's cases will participate in regular meetings with other State and federal government agencies such as the West Virginia Office of the Insurance Commissioner (OIC), the West Virginia Medicaid Fraud Control Unit (MFCU), United States Attorney's Offices, and County Prosecuting Attorneys upon request and as needed to protect PEIA's financial interests and ensure accountability for criminal violations by PEIA members, providers, and/or contractors.		
5.1.22	Vendor will perform statistically valid random sampling (SVRS) and mathematical extrapolation of overpayments across a provider's wider billing universe based on SVRS findings in accordance with recognized federal standards.		

5.1.23	Vendor must confirm and agree that any and/or all data received from PEIA and/or used by the Vendor shall be kept secure in accordance with applicable provisions of the HIPAA Security Rule(s) and applicable NIST Standards and/or Guidance including, but not limited to, appropriate security and encryption when being transmitted and when at rest.		
5.1.24	Vendor must guarantee a minimum Return On Investment (ROI) from its services no less than 2:1. The methodology to determine ROI must be clear and well defined.		
5.1.25	Vendor must agree that all data collected, created, shared, or generated under the scope of work of this contract will be kept secured, encrypted, and segregated in a manner so that, if needed and/or upon termination of the contract it can be rendered unreadable, unusable or indecipherable or otherwise destroyed in accordance with applicable provisions of the HIPAA Security Rules. The referenced data is the sole property of the West Virginia Public Employees Insurance Agency (PEIA) and may not be used for any other projects, contracts, or purposes without the express written consent of PEIA. Any severance or change in status of a subcontractor, employee, collaborator, student, or agent, whether voluntary or involuntary, shall immediately terminate their rights to access, use, or otherwise have direct or indirect permissions with regard to said data. Under no circumstances will any PEIA data, neither in an identified form nor in a deidentified format, be stored, transmitted/sent, used, or otherwise viewed outside the Continental United States. PEIA data may only be used for the fulfillment of the scope of work under the proposed contract or Agreement and may not be used for any other purpose.		
5.1.26	The vendor must utilize systems/software that support a secure data management structure that is compliant with any and/or all State and/or federal security and privacy laws, rules, regulations, and/or standards.		
5.1.27	Vendor agrees, confirms, and understands that any contract or award made under this solicitation shall be governed by the laws of the State of West Virginia.		

5.2 MINIMUM VENDOR REQUIREMENTS			
SECTION	REQUIREMENT	CONFIRM/ DO NOT CONFIRM	ADDITIONAL INFORMATION IF DEVIATING
5.2.1	Vendor shall provide information and documentation in **Attachment 14 (Staff Resumes)** regarding the firm's staff qualifications and experience in performing post payment medical and pharmaceutical claim review services and conducting healthcare FWA investigations as described in Section 4.2 above.		
5.2.2	Vendor shall submit a company summary including company history, office location(s), company size, financial summary from most recent fiscal year (including total revenue, total liabilities, total assets, and net margin not to exceed four (4) pages), and statement of technical areas of expertise. The Vendor must be able to substantiate that the Vendor has sufficient resources to complete the project successfully within the time requirements.		
5.2.3	Vendor shall provide at least 3 active client references and 3 terminated client references in **Attachment 13 (Vendor Experience)**. Vendor may substitute additional active client references for the 3 terminated client references, but Vendor must submit at least 6 total client references.		
5.2.4	Vendor shall provide the following Financials and Ratings information: • Certificate of Insurance • Financial statements • Accreditations, if any • Financial ratings, if any		
5.2.5	Vendor will provide a list of any current subcontractors, collaborators, and other third parties that will perform duties under this contract, including firm name and address, contact person, complete description of work to be subcontracted, and descriptive information concerning subcontractor's organizational abilities. This information will be provided with the bid proposal in **Attachment 12 (Subcontractor Information Form)**.		
5.2.6	Vendor must demonstrate a minimum of four (4) years of experience conducting complex healthcare FWA investigations as evidenced by contracts in place for at least five (5) years, at least two (2) years of which include conducting complex healthcare fraud investigations for a health plan client with at least 50,000 covered lives.		

5.2.7	Vendor shall provide information and demonstrate that it has experience conducting complex healthcare FWA investigations involving providers in rural areas. Vendor may demonstrate this experience by listing clients as a reference or providing evidence of such investigations that Vendor successfully completed including the results obtained from such investigations.		
5.2.8	Vendor must be, and must remain, compliant with all federal regulations impacting healthcare fraud investigations, including but not limited to compliance with HIPAA and all related privacy and security regulations.		
5.2.9	Vendor must agree to immediately (no more than one (1) business day) report any event or incident that may result in any real or perceived harm to any member, provider, or the Agency.		
5.2.10	The vendor shall agree in accordance with applicable provisions of 45 CFR § 164.512(e)(1)(i) and (f)(1)(ii), the vendor, or any subcontractor of the vendor, is required to notify PEIA within five (5) business days if it is involved or engaged in any litigation which can or may result in the disclosure or re-disclosure of any PEIA member PII/PHI in an identified or de-identified format. The State of West Virginia and PEIA reserve the right to defend against any such disclosures or re-disclosures.		
5.2.11	Vendor must have at least one (1) staff member assigned to work on PEIA's cases who is a full-time resident of West Virginia and possesses at least three (3) years of professional experience working on healthcare FWA investigations.		
5.2.12	Vendor must have demonstrated experience coordinating with a commercial or public sector health plan's TPA, PBM, and data warehouse vendor to obtain access to claims data in a secure manner that complies with any and/or all State and/or federal security and privacy laws, rules, regulations, and/or standards.		
5.2.13	Vendor shall identify any projects within the last ten (10) years where the Contract in question was cancelled, terminated for cause, or any litigation related to Vendor's past performance was initiated.		
5.2.14	Vendor shall supply an attestation (written documentation) of a favorable background check, at the expense of the Vendor for Vendor personnel who might reasonably be expected to access sensitive and confidential client data contained in any system accessed during the Contract. The Agency may request the removal of staff for disqualifying offenses.		

5.3 MINIMUM PERFORMANCE GUARANTEES			
SECTION	REQUIREMENT	CONFIRM/ DO NOT CONFIRM	ADDITIONAL INFORMATION IF DEVIATING
5.3.1	It is PEIA's intention and expectation that the savings achieved through this solicitation shall more than cover the costs of the Vendor's services. As described in Section 5.1.24 above, the Vendor must guarantee a minimum Return On Investment (ROI) from its services no less than 2:1. The methodology to determine ROI must be clear and well defined.		

Vendor's signature below certifies that all of the mandatory minimum requirements in Section 5 have been carefully evaluated and understood, and Vendor meets or agrees to each item.

_____
(Company)

_____
(Representative Name, Title)

_____
(Date)

Attachment 4
Vendor Registration Requirements

Vendors must complete all three registrations below before an award document can be finalized. Registration is not required for bidding.

Vendors may register with the WV Secretary of State and the WV Tax Department simultaneously at http://www.business4wv.com, but **wvOasis Vendor Registration is a separate and distinct process**.

WV STATE VENDOR REGISTRATION - WVOASIS

Vendors doing business with the State of West Virginia are required to register with wvOasis. This consists of [at minimum]: (A) registration in the VSS system (either manually or by paper application), (B) submission of a W-9 to the State Finance Division, (C) disclosure of at least two officers and banking information. and (D) payment of a $125 annual vendor registration fee [*Certain exemptions to the fee apply. Information below*]

Vendors may register in one of the following ways:

1. Vendor Self Service (VSS)

   VSS Link: https://prod-fin-vss.wvoasis.gov/webapp/prdvss11/AltSelfService

   VSS FAQ: http://www.state.wv.us/admin/purchase/VendorReg.html

   Help: wvOasis Help Desk
   helpdesk@wvoasis.gov
   304-558-6708

2. Vendor Registration and Disclosure Statement and Small, Women-, and Minority-Owned Business Certification Application

   Download: http://www.state.wv.us/admin/purchase/vrc/wv1.pdf

   Send to: Purchasing Division - Vendor Registration
   2019 Washington Street East
   Charleston, WV 25305-0130

Exemption to the $125 Vendor Registration Fee - In specific situations, the fee may be waived for vendors providing goods/services to the State of West Virginia. This exemption only applies to specific transactions. If a vendor provides an exempt service, but then wishes to provide a non-exempt service, they are required to pay the registration fee before an award can be made for a non-exempt service.

Some vendor services commodities/services solicited by PEIA will qualify for this exemption. If a vendor is unsure whether they need to pay the fee, they can contact the PEIA Procurement Officer or the RFP Coordinator of the Solicitation they are reviewing.

WV SECRETARY OF STATE REGISTRATION

Registration with the WV Secretary of State's Office is required for all Vendors doing business with the State of West Virginia, and may require a fee of $100.00 depending on the business registration category.

Business registration with the Secretary of State falls into one of the two categories:

a. Domestic (formed in West Virginia), or
b. Foreign (formed out-of-state)

Vendors may complete an Application for Exemption from Certificate of Authority with the WV SOS if you feel your company qualifies. Please mail the completed form and include a check for $25.00, made payable to WV SOS, along with a copy of the company's home state issued Certificate of Good Standing / Certificate of Corporation.

http://www.sos.wv.gov/business-licensing/forms/Documents/Corporation/cf-2.pdf

You may contact the WV Secretary of State's Office with your questions @ 304-558-6000

WV TAX DEPARTMENT

All entities doing business in the State of West Virginia must be registered with WV TAX and pay a one-time fee of $30.00.

An exemption with the WV Secretary of State does not mean you are exempt from registering with the WV Tax Department.

If you need to speak to someone at the WV Tax Department, please call 304-558-8683.

NOTE:

You may use the Business4WV website to register with the WV Secretary of State and the WV Tax Department simultaneously at http://www.business4wv.com. Please note there is a one-time fee of $130.00.

Attachment 5

WV State Invoice Requirements

Vendor invoices must contain the correct information before being presented to the State for payment. Failure to include any required elements will delay payment until the vendor sends a corrected invoice to PEIA. The full Legislative Rule can b e found in "Rules for Auditing - title 155-01", available at https://www.wvsao.gov/Auditing/Default.

Common issues that delay payment:

Vendor Information - Vendor name and remit-to address must appear on the invoice. This information must match exactly what is in the wvOasis system. This includes any name add-ons such as "Inc." or "LLC".

Itemization - Detailed itemization of all charges must be included. This includes specific dates of service, if necessary, or copies of receipts/receiving reports from third party transactions if necessary.

Contract Award Information - Reference to the specific contract award should be included to expedite payment. This includes the Contract Award Number (i.e. AMA PEIxxxxxxxxxx, ACT PEIxxxxxxxxxx, etc), Change Order number if applicable, and specific commodity/service line number.

Any questions regarding invoice requirements can be directed to **PEIAAccountsPayable@wv.gov**

All invoices should be submitted to **PEIAAccountsPayable@wv.gov**

Attachment 6
WV-96 Form

FINAL CONTRACT WILL NOT BE NEGOTIATED UNTIL THIS ADDENDUM IS FULLY EXECUTED.

SEE ATTACHED FORM

WV-96
1/1/2019

STATE OF WEST VIRGINIA
ADDENDUM TO VENDOR'S STANDARD CONTRACTUAL FORMS

State Agency, Board, or Commission (the "State"):

Vendor:

Contract/Lease Number ("Contract"):

Commodity/Service:

The State and the Vendor are entering into the Contract identified above. The Vendor desires to incorporate one or more forms it created into the Contract. Vendor's form(s), however, include(s) one or more contractual terms and conditions that the State cannot or will not accept. In consideration for the State's incorporating Vendor's form(s) into the Contract, the Vendor enters into this Addendum which specifically eliminates or alters the legal enforceability of certain terms and conditions contained in Vendor's form(s). Therefore, on the date shown below each signature line, the parties agree to the following contractual terms and conditions in this Addendum are dominate over any competing terms made a part of the Contract:

1. **ORDER OF PRECEDENCE:** This Addendum modifies and supersedes anything contained on Vendor's form(s) whether or not they are submitted before or after the signing of this Addendum. IN THE EVENT OF ANY CONFLICT BETWEEN VENDOR'S FORM(S) AND THIS ADDENDUM, THIS ADDENDUM SHALL CONTROL.

2. **PAYMENT** – Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software licenses, subscriptions, or maintenance may be paid annually in advance.

   Any language imposing any interest or charges due to late payment is deleted.

3. **FISCAL YEAR FUNDING** – Performance of this Contract is contingent upon funds being appropriated by the WV Legislature or otherwise being available for this Contract. In the event funds are not appropriated or otherwise available, the Contract becomes of no effect and is null and void after June 30 of the current fiscal year. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

4. **RIGHT TO TERMINATE** – The State reserves the right to terminate this Contract upon thirty (30) days written notice to the Vendor. If this right is exercised, the State agrees to pay the Vendor only for all undisputed services rendered or goods received before the termination's effective date. All provisions are deleted that seek to require the State to (1) compensate Vendor, in whole or in part, for lost profit, (2) pay a termination fee, or (3) pay liquidated damages if the Contract is terminated early.

   Any language seeking to accelerate payments in the event of Contract termination, default, or non-funding is hereby deleted.

5. **DISPUTES** – Any language binding the State to any arbitration or to the decision of any arbitration board, commission, panel or other entity is deleted; as is any requirement to waive a jury trial.

   Any language requiring or permitting disputes under this Contract to be resolved in the courts of any state other than the State of West Virginia is deleted. All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

   Any language requiring the State to agree to, or be subject to, any form of equitable relief not authorized by the Constitution or laws of State of West Virginia is deleted.

6. **FEES OR COSTS:** Any language obligating the State to pay costs of collection, court costs, or attorney's fees, unless ordered by a court of competent jurisdiction is deleted.

7. **GOVERNING LAW** – Any language requiring the application of the law of any state other than the State of West Virginia in interpreting or enforcing the Contract is deleted. The Contract shall be governed by the laws of the State of West Virginia.

8. **RISK SHIFTING** – Any provision requiring the State to bear the costs of all or a majority of business/legal risks associated with this Contract, to indemnify the Vendor, or hold the Vendor or a third party harmless for any act or omission is hereby deleted.

9. **LIMITING LIABILITY** – Any language limiting the Vendor's liability for direct damages to person or property is deleted.

10. **TAXES** – Any provisions requiring the State to pay Federal, State or local taxes or file tax returns or reports on behalf of Vendor are deleted. The State will, upon request, provide a tax exempt certificate to confirm its tax exempt status.

11. **NO WAIVER** – Any provision requiring the State to waive any rights, claims or defenses is hereby deleted.

12. **STATUTE OF LIMITATIONS** – Any clauses limiting the time in which the State may bring suit against the Vendor or any other third party are deleted.

13. **ASSIGNMENT** – The Vendor agrees not to assign the Contract to any person or entity without the State's prior written consent, which will not be unreasonably delayed or denied. The State reserves the right to assign this Contract to another State agency, board or commission upon thirty (30) days written notice to the Vendor. These restrictions do not apply to the payments made by the State. Any assignment will not become effective and binding upon the State until the State is notified of the assignment, and the State and Vendor execute a change order to the Contract.

14. **RENEWAL** – Any language that seeks to automatically renew, modify, or extend the Contract beyond the initial term or automatically continue the Contract period from term to term is deleted. The Contract may be renewed or continued only upon mutual written agreement of the Parties.

15. **INSURANCE** – Any provision requiring the State to maintain any type of insurance for either its or the Vendor's benefit is deleted.

16. **RIGHT TO REPOSSESSION NOTICE** – Any provision for repossession of equipment without notice is hereby deleted. However, the State does recognize a right of repossession with notice.

17. **DELIVERY** – All deliveries under the Contract will be FOB destination unless the State expressly and knowingly agrees otherwise. Any contrary delivery terms are hereby deleted.

18. **CONFIDENTIALITY** – Any provisions regarding confidential treatment or non-disclosure of the terms and conditions of the Contract are hereby deleted. State contracts are public records under the West Virginia Freedom of Information Act ("FOIA") (W. Va. Code §29B-a-1, et seq.) and public procurement laws. This Contract and other public records may be disclosed without notice to the vendor at the State's sole discretion.

    Any provisions regarding confidentiality or non-disclosure related to contract performance are only effective to the extent they are consistent with FOIA and incorporated into the Contract through a separately approved and signed non-disclosure agreement.

19. **THIRD-PARTY SOFTWARE** – If this Contract contemplates or requires the use of third-party software, the vendor represents that none of the mandatory click-through, unsigned, or web-linked terms and conditions presented or required before using such third-party software conflict with any term of this Addendum or that is has the authority to modify such third-party software's terms and conditions to be subordinate to this Addendum. The Vendor shall indemnify and defend the State against all claims resulting from an assertion that such third-party terms and conditions are not in accord with, or subordinate to, this Addendum.

20. **AMENDMENTS** – The parties agree that all amendments, modifications, alterations or changes to the Contract shall be by mutual agreement, in writing, and signed by both parties. Any language to the contrary is deleted.

    Notwithstanding the foregoing, this Addendum can only be amended by (1) identifying the alterations to this form by using *Italics* to identify language being added and ~~strikethrough~~ for language being deleted (do not use track-changes) and (2) having the Office of the West Virginia Attorney General's authorized representative expressly agree to and knowingly approve those alterations.

State: _____	Vendor: _____
By: _____	By: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Attachment 7
DATA MANAGEMENT ADDENDUM & APPENDIX

NOTE: THE TERMS OF THE DATA MANAGEMENT ADDENDUM ARE NON-NEGOTIABLE AND MUST BE EXECUTED AS-IS IN ANY EVENTUAL CONTRACT RESULTING FROM THIS RFP

FINAL CONTRACT WILL NOT BE NEGOTIATED UNTIL THIS ADDENDUM IS FULLY EXECUTED.

SEE ATTACHED FORM

Data Exchange – Data Management Addendum

1. Definitions:

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Business Associate is any person or company—other than a covered entity's workforce—that creates, receives, maintains, or transmits protected health information (PHI) on behalf of a covered entity, as defined in 45 CFR §160.103. This includes, but is not necessarily limited to vendors such as TPAs, PBMs, auditors, billing companies, EHR providers, cloud storage services, and legal or accounting firms that access PHI.

Covered Entity means a HIPAA covered entity such as a health plan, a health care clearinghouse, or a health care provider that transmits health information electronically in a HIPAA-standard transaction, as defined at 45 CFR §160.103.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Governing Law – The terms and conditions of the Data Exchange – Data Management Addendum shall be governed by the laws of the State of West Virginia and/or of the United States and shall not be subject to any other sovereign.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information,

including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. §1232g, records described at 20 U.S.C. §1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A, the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.

c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.

e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.

f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.

g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the West Virginia Public Employees Insurance Agency and its end users solely from data centers in the United States. Storage of public jurisdiction data at rest shall be located solely in data centers in the United States. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its data centers within the United States. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.

b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.

c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.

c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.

d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public

jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.

b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.

c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.
e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or

approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:

a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.

c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services

being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

a. Access and use the service for its business purposes;
b. For SaaS, use underlying software as embodied or used in the service; and
c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and

any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

For WV PEIA:_____	Name of Vendor:_____
Signature:_____	Signature:_____
Title:_____	Title:_____
Date:_____	Date:_____

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: _____

Name of Agency:_____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes ☐
   No ☐

2. If yes to #1, does the restricted information include personal data?
   Yes ☐
   No ☐

3. If yes to #1, does the restricted information include non-public data?
   Yes ☐
   No ☐

4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes ☐
   No ☐

5. Provide name and email address for the Department privacy officer:

   Name: _____

   Email address: _____

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

   Name: _____

   Email address: _____

   Phone Number: _____ _____

Attachment 8
HIPAA BUSINESS ASSOCIATE ADDENDUM & APPENDIX

FINAL CONTRACT WILL NOT BE NEGOTIATED UNTIL THIS ADDENDUM IS FULLY EXECUTED.

SEE ATTACHED FORM

WV STATE GOVERNMENT

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Health Insurance Portability and Accountability Act of 1996 (hereafter, HIPAA) Business Associate Addendum ("Addendum") is made a part of the Agreement ("Agreement") by and between the State of West Virginia ("Agency"), and Business Associate ("Associate"), and is effective as of the date of execution of the Addendum.

The Associate performs certain services on behalf of or for the Agency pursuant to the underlying Agreement that requires the exchange of information including protected health information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA"). The Agency is a "Covered Entity" as that term is defined in HIPAA, and the parties to the underlying Agreement are entering into this Addendum to establish the responsibilities of both parties regarding HIPAA-covered information and to bring the underlying Agreement into compliance with HIPAA.

Whereas it is desirable, in order to further the continued efficient operations of Agency to disclose to its Associate certain information which may contain confidential individually identifiable health information (hereafter, Protected Health Information or PHI); and

Whereas, it is the desire of both parties that the confidentiality of the PHI disclosed hereunder be maintained and treated in accordance with all applicable laws relating to confidentiality, including the Privacy and Security Rules, the HITECH Act and its associated regulations, and the parties do agree to at all times treat the PHI and interpret this Addendum consistent with that desire.

NOW THEREFORE: the parties agree that in consideration of the mutual promises herein, in the Agreement, and of the exchange of PHI hereunder that:

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

    a. **Agency Procurement Officer** shall mean the appropriate Agency individual listed at: http://www.state.wv.us/admin/purchase/vrc/agencyli.html.

    b. **Agent** shall mean those person(s) who are agent(s) of the Business Associate, in accordance with the Federal common law of agency, as referenced in 45 CFR § 160.402(c).

    c. **Breach** shall mean the acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except as excluded in the definition of Breach in 45 CFR § 164.402.

    d. **Business Associate** shall have the meaning given to such term in 45 CFR § 160.103.

    e. **HITECH Act** shall mean the Health Information Technology for Economic and Clinical Health Act. Public Law No. 111-05. 111th Congress (2009).

f. **Privacy Rule** means the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Parts 160 and 164.

g. **Protected Health Information or PHI** shall have the meaning given to such term in 45 CFR § 160.103, limited to the information created or received by Associate from or on behalf of Agency.

h. **Security Incident** means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information or interference with system operations in an information system.

i. **Security Rule** means the Security Standards for the Protection of Electronic Protected Health Information found at 45 CFR Parts 160 and 164.

j. **Subcontractor** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

2. **Permitted Uses and Disclosures.**

a. **PHI Described.** This means PHI created, received, maintained or transmitted on behalf of the Agency by the Associate. This PHI is governed by this Addendum and is limited to the minimum necessary, to complete the tasks or to provide the services associated with the terms of the original Agreement, and is described in Appendix A.

b. **Purposes.** Except as otherwise limited in this Addendum, Associate may use or disclose the PHI on behalf of, or to provide services to, Agency for the purposes necessary to complete the tasks, or provide the services, associated with, and required by the terms of the original Agreement, or as required by law, if such use or disclosure of the PHI would not violate the Privacy or Security Rules or applicable state law if done by Agency or Associate, or violate the minimum necessary and related Privacy and Security policies and procedures of the Agency. The Associate is directly liable under HIPAA for impermissible uses and disclosures of the PHI it handles on behalf of Agency.

c. **Further Uses and Disclosures**. Except as otherwise limited in this Addendum, the Associate may disclose PHI to third parties for the purpose of its own proper management and administration, or as required by law, provided that (i) the disclosure is required by law, or (ii) the Associate has obtained from the third party reasonable assurances that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party by the Associate; and, (iii) an agreement to notify the Associate and Agency of any instances of which it (the third party) is aware in which the confidentiality of the information has been breached. To the extent practical, the information should be in a limited data set or the minimum necessary information pursuant to 45 CFR § 164.502, or take other measures as necessary to satisfy the Agency's obligations under 45 CFR § 164.502.

3. **Obligations of Associate.**

a. **Stated Purposes Only.** The PHI may not be used by the Associate for any purpose other than as stated in this Addendum or as required or permitted by law.

b. **Limited Disclosure.** The PHI is confidential and will not be disclosed by the Associate other than as stated in this Addendum or as required or permitted by law. Associate is prohibited from directly or indirectly receiving any remuneration in exchange for an individual's PHI unless Agency gives written approval and the individual provides a valid authorization. Associate will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act. Associate will report to Agency any use or disclosure of the PHI, including any Security Incident not provided for by this Agreement of which it becomes aware.

c. **Safeguards.** The Associate will use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of the PHI, except as provided for in this Addendum. This shall include, but not be limited to:

i. Limitation of the groups of its workforce and agents, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Addendum, and the use and disclosure of the minimum PHI necessary or a Limited Data Set;

ii. Appropriate notification and training of its workforce and agents in order to protect the PHI from unauthorized use and disclosure;

iii. Maintenance of a comprehensive, reasonable and appropriate written PHI privacy and security program that includes administrative, technical and physical safeguards appropriate to the size, nature, scope and complexity of the Associate's operations, in compliance with the Security Rule;

iv. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

d. **Compliance With Law.** The Associate will not use or disclose the PHI in a manner in violation of existing law and specifically not in violation of laws relating to confidentiality of PHI, including but not limited to, the Privacy and Security Rules.

e. **Mitigation.** Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Associate of a use or disclosure of the PHI by Associate in violation of the requirements of this Addendum, and report its mitigation activity back to the Agency.

f. **Support of Individual Rights.**

i. **Access to PHI.** Associate shall make the PHI maintained by Associate or its agents or subcontractors in Designated Record Sets available to Agency for inspection and copying, and in electronic format, if requested, within ten (10) days of a request by Agency to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.524 and consistent with Section 13405 of the HITECH Act.

ii. **Amendment of PHI.** Within ten (10) days of receipt of a request from Agency for an amendment of the PHI or a record about an individual contained in a Designated Record Set, Associate or its agents or subcontractors shall make such PHI available to Agency for amendment and incorporate any such amendment to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.526.

iii. **Accounting Rights.** Within ten (10) days of notice of a request for an accounting of disclosures of the PHI, Associate and its agents or subcontractors shall make available to Agency the documentation required to provide an accounting of disclosures to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR §164.528 and consistent with Section 13405 of the HITECH Act. Associate agrees to document disclosures of the PHI and information related to such disclosures as would be required for Agency to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. This should include a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years from the date of disclosure, or longer if required by state law. At a minimum, such documentation shall include:

- the date of disclosure;
- the name of the entity or person who received the PHI, and if known, the address of the entity or person;
- a brief description of the PHI disclosed; and
- a brief statement of purposes of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.

iv. **Request for Restriction**. Under the direction of the Agency, abide by any individual's request to restrict the disclosure of PHI, consistent with the requirements of Section 13405 of the HITECH Act and 45 CFR § 164.522, when the Agency determines to do so (except as required by law) and if the disclosure is to a health plan for payment or health care operations and it pertains to a health care item or service for which the health care provider was paid in full "out-of-pocket."

v. **Immediate Discontinuance of Use or Disclosure.** The Associate will immediately discontinue use or disclosure of Agency PHI pertaining to any individual when so requested by Agency. This includes, but is not limited to, cases in which an individual has withdrawn or modified an authorization to use or disclose PHI.

g. **Retention of PHI.** Notwithstanding section 4.a. of this Addendum, Associate and its subcontractors or agents shall retain all PHI pursuant to state and federal law and shall continue to maintain the PHI required under Section 3.f. of this Addendum for a period of six (6) years after termination of the Agreement, or longer if required under state law.

h. **Agent's, Subcontractor's Compliance.** The Associate shall notify the Agency of all subcontracts and agreements relating to the Agreement, where the subcontractor or agent receives PHI as described in section 2.a. of this Addendum. Such notification shall occur within 30 (thirty) calendar days of the execution of the subcontract and shall be delivered to the Agency Procurement Officer. The Associate will ensure that any of its subcontractors, to whom it provides any of the PHI it receives hereunder, or to whom it provides any PHI which the Associate creates or receives on behalf of the Agency, agree to the restrictions and conditions which apply to the Associate hereunder. The Agency may request copies of downstream subcontracts and agreements to determine whether all restrictions, terms and conditions have been flowed down. Failure to ensure that downstream contracts, subcontracts and agreements contain the required restrictions, terms and conditions may result in termination of the Agreement.

j. **Federal and Agency Access.** The Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI, as well as the PHI, received from, or created or received by the Associate on behalf of the Agency available to the U.S. Secretary of Health and Human Services consistent with 45 CFR § 164.504. The Associate shall also make these records available to Agency, or Agency's contractor, for periodic audit of Associate's compliance with the Privacy and Security Rules. Upon Agency's request, the Associate shall provide proof of compliance with HIPAA and HITECH data privacy/protection guidelines, certification of a secure network and other assurance relative to compliance with the Privacy and Security Rules. This section shall also apply to Associate's subcontractors, if any.

k. **Security.** The Associate shall take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. In addition, compliance with 74 FR 19006 Guidance Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII is required, to the extent practicable. If Associate chooses not to adopt such methodologies as defined in 74 FR 19006 to secure the PHI governed by this Addendum, it must submit such written rationale, including its Security Risk Analysis, to the Agency Procurement Officer for review prior to the execution of the Addendum. This review may take up to ten (10) days.

l. **Notification of Breach.** During the term of this Addendum, the Associate shall notify the Agency and, unless otherwise directed by the Agency in writing, the WV Office of Technology immediately by e-mail or web form upon the discovery of any Breach of unsecured PHI; or within 24 hours by e-mail or web form of any suspected Security Incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the Agency Procurement Officer at www.state.wv.us/admin/purchase/vrc/agencyli.htm and,

unless otherwise directed by the Agency in writing, the Office of Technology at incident@wv.gov or https://apps.wv.gov/ot/ir/Default.aspx.

The Associate shall immediately investigate such Security Incident, Breach, or unauthorized use or disclosure of PHI or confidential data. Within 72 hours of the discovery, the Associate shall notify the Agency Procurement Officer, and, unless otherwise directed by the Agency in writing, the Office of Technology of: (a) Date of discovery; (b) What data elements were involved and the extent of the data involved in the Breach; (c) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data; (d) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized; (e) A description of the probable causes of the improper use or disclosure; and (f) Whether any federal or state laws requiring individual notifications of Breaches are triggered.

Agency will coordinate with Associate to determine additional specific actions that will be required of the Associate for mitigation of the Breach, which may include notification to the individual or other authorities.

All associated costs shall be borne by the Associate. This may include, but not be limited to costs associated with notifying affected individuals.

If the Associate enters into a subcontract relating to the Agreement where the subcontractor or agent receives PHI as described in section 2.a. of this Addendum, all such subcontracts or downstream agreements shall contain the same incident notification requirements as contained herein, with reporting directly to the Agency Procurement Officer. Failure to include such requirement in any subcontract or agreement may result in the Agency's termination of the Agreement.

m. **Assistance in Litigation or Administrative Proceedings.** The Associate shall make itself and any subcontractors, workforce or agents assisting Associate in the performance of its obligations under this Agreement, available to the Agency at no cost to the Agency to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Agency, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inaction or actions by the Associate, except where Associate or its subcontractor, workforce or agent is a named as an adverse party.

4. Addendum Administration.

a. **Term.** This Addendum shall terminate on termination of the underlying Agreement or on the date the Agency terminates for cause as authorized in paragraph (c) of this Section, whichever is sooner.

b. **Duties at Termination.** Upon any termination of the underlying Agreement, the Associate shall return or destroy, at the Agency's option, all PHI received from, or created or received by the Associate on behalf of the Agency that the Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, the Associate shall extend the protections of this Addendum to the PHI and limit further uses and disclosures to the purposes that make the return or destruction of the PHI infeasible. This shall also apply to all agents and subcontractors of Associate. The duty of the Associate and its agents

and subcontractors to assist the Agency with any HIPAA required accounting of disclosures survives the termination of the underlying Agreement.

c. **Termination for Cause.** Associate authorizes termination of this Agreement by Agency, if Agency determines Associate has violated a material term of the Agreement. Agency may, at its sole discretion, allow Associate a reasonable period of time to cure the material breach before termination.

d. **Judicial or Administrative Proceedings.** The Agency may terminate this Agreement if the Associate is found guilty of a criminal violation of HIPAA. The Agency may terminate this Agreement if a finding or stipulation that the Associate has violated any standard or requirement of HIPAA/HITECH, or other security or privacy laws is made in any administrative or civil proceeding in which the Associate is a party or has been joined. Associate shall be subject to prosecution by the Department of Justice for violations of HIPAA/HITECH and shall be responsible for any and all costs associated with prosecution.

e. **Survival.** The respective rights and obligations of Associate under this Addendum shall survive the termination of the underlying Agreement.

5. **General Provisions/Ownership of PHI.**

a. **Retention of Ownership.** Ownership of the PHI resides with the Agency and is to be returned on demand or destroyed at the Agency's option, at any time, and subject to the restrictions found within section 4.b. above.

b. **Secondary PHI.** Any data or PHI generated from the PHI disclosed hereunder which would permit identification of an individual must be held confidential and is also the property of Agency.

c. **Electronic Transmission.** Except as permitted by law or this Addendum, the PHI or any data generated from the PHI which would permit identification of an individual must not be transmitted to another party by electronic or other means for additional uses or disclosures not authorized by this Addendum or to another contractor, or allied agency, or affiliate without prior written approval of Agency.

d. **No Sales.** Reports or data containing the PHI may not be sold without Agency's or the affected individual's written consent.

e. **No Third-Party Beneficiaries.** Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Agency, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

f. **Interpretation.** The provisions of this Addendum shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provisions in this Addendum. The interpretation of this Addendum shall be made under the laws of the state of West Virginia.

g. **Amendment.** The parties agree that to the extent necessary to comply with applicable law they will agree to further amend this Addendum.

h. **Additional Terms and Conditions.** Additional discretionary terms may be included in the release order or change order process.

AGREED:

Name of Agency:_____

Signature:_____

Title:_____

Date:_____

Name of Associate:_____

Signature:_____

Title:_____

Date:_____

Form - WVBAA-012004
Amended 06.26.2013

APPROVED AS TO FORM THIS 26th
DAY Of June 20 13
Patrick Morrisey
Attorney General
BY _____

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. PHI not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Associate: _____

Name of Agency: _____

Describe the PHI (do not include any actual PHI). If not applicable, please indicate the same.

Appendix A

Name of Associate: **Health Insurance Special Investigations of Fraud, Waste, and Abuse Vendor**

Name of Agency(ies) (Covered Entity): **The West Virginia Public Employees Insurance Agency (PEIA)**

Describe the PHI. If not applicable please indicate the same.

Per 45 CFR, Part 160.103

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

In any and/or all circumstances, only the minimum necessary PHI will be shared by the Covered Entity to the Associate for the meaningful use as outlined in the scope of work of the Master Agreement between the parties.

Nothing in this document shall transfer, assign, and/or convey any ownership rights and/or privileges of and/or for the data from the Covered Entity to the Associate. Any and/or all data released to the Associate by the Covered Entity shall remain the sole property of the Covered Entity and/or the State of West Virginia.

Any and/or all data shared by the Covered Entity to the Associate shall remain within the continental United States and shall not under any circumstances leave United States jurisdiction.

In partnership with the Covered Entity (PEIA), the Plan's Third Party Administrator, the Plan's HMO Vendor and the Pharmacy Benefit Manager (PBM), will provide the Health Insurance Special Investigations of Fraud, Waste, and Abuse Vendor the medical and/or pharmacy and/or drug claims information necessary to perform the Scope of Work as outlined in the Agreement. The following protected health information will be released to the Associate to facilitate the performance of the scope of work as outlined in the Agreement:

a) PEIA member and dependent name(s), date(s) of birth, policy number(s), benefit tier(s), and other necessary demographic data needed to properly assign benefit(s) and formulary(ies).
b) Access to the Covered Entity's medical claims record(s) system for the meaningful use of performing queries; conducting claims analytics; utilizing software or tools to review claims and/or claims patterns, and; otherwise look for patterns indicative of fraud, waste, and abuse.
c) PEIA member and dependent medical, pharmacy and/or specialty pharmacy claims data including date, type of service, procedure code(s), billing, rate(s), provider information, diagnosis, etc. needed to perform the Scope of Work as outlined in the Agreement.
d) PEIA member and dependent medical, pharmacy and/or specialty pharmacy claims data as it directly relates to benefit service utilization and/or payment(s).
e) The Associate shall comply with any and/or all provisions of Titles I & II of the Health Insurance Portability and Accountability Act of 1996, Pub.L. 104–191, 110 Stat. 1936, as amended, and the Health Information Technology for Economic and Clinical Health Act (HITECH) enacted as part of the American Reinvestment and Reauthorization Act of 2009 (ARRA), including the Final Omnibus Rule.
f) In all instances, only the minimum amount of PHI necessary for the Associate to complete the scope of work under this contract shall be released to the Associate pursuant to the Agreement.

Attachment 9
BIDDERS LITIGATION WAIVER FORM

_____, hereinafter "Bidder," wishes to submit a Bid in response to the Request for Proposal for Outpatient Pharmacy Cost Containment Services issued by the Public Employees Insurance Agency for the State of West Virginia (PEIA). The Bidder acknowledges that a mandatory requirement of the RFP is that the Bidder submit a litigation bond or waiver with its proposal.

In consideration of the waiver of said litigation bond requirement by the PEIA, and in lieu of such bond, the Bidder agrees:

That the Bidder completely waives and forgoes any and all legal right or ability it may now have, or in the future, ot initiate any sort of challenge to or against the selection of a Bidder and/or the ultimate award of a contract or contracts pursuant to the RFP. This Waiver is entered voluntarily by a representative authorized to legally bind the Bidder and shall be binding on the Bidder, its successors, assigns, heirs and any others claiming under the legal rights of the Bidder. This Waiver shall apply to any and all types of action, in challenge to or seeking to attack, in any way, the RFP selection process, or the subsequent award of contract(s) to the successful Bidder, including but not limited to, administrative, judicial, or collateral actions.

LEGAL NAME OF BIDDER

AUTHORIZED SIGNATURE	
TITLE	**DATE**

APPROVED:

PUBLIC EMPLOYEES INSURANCE AGENCY FOR THE STATE OF WEST VIRGINIA

AUTHORIZED SIGNATURE	
TITLE	**DATE**

Attachment 10
REDACTION ATTESTATION FORM

This RFP, any bid proposals, and any resulting contract is subject to public disclosure under the West Virginia Freedom of Information Act ("FIOA"). Accordingly, if the Bidder considers any part of its bid proposal to contain secret information exempt from disclosure under FOIA then the Bidder must provide a second, redacted copy of its bid proposal in conjunction with the original bid proposal. Wee W. Va. Code §29B-1-4.

For purposes of redaction, the vendor must be specific as to why a FOIA exemption applies. Redactions m ust be "surgical" and not "global", i.e. redaction of the number(s) after a percentage (%) or a price ($) mark and not redactions of whole paragraphs or pages. Bidder(s) shall assume any and/or all response for the defense of the non-release of the Bid submission(s) under FOIA statute(s). The PEIA assumes no responsibility nor liability for making nor defending the redactions to any bid proposal or submission defending any release under FOIA

See also W. Va. Code §47-22-1(d).

LEGAL NAME OF BIDDER

AUTHORIZED SIGNATURE	
TITLE	**DATE**

Attachment 11
MASTER SERVICE AGREEMENT

SEE ATTACHED FORM

WEST VIRGINIA PUBLIC EMPLOYEES INSURANCE AGENCY

MASTER SERVICE AGREEMENT

This document shall serve as the Master Level Service Agreement between the West Virginia Public Employees Insurance Agency (PEIA) and _____, hereafter referred to as the "Vendor", for the provision of services in whole or in part to and for PEIA's member population. PEIA and the Vendor, hereafter referred to as the "Parties" hereby agree to the following:

RECITALS

WHEREAS, PEIA provides health insurance benefits to statutorily eligible employer groups and their covered person(s) in the State of West Virginia under West Virginia Code §5-16-1 et. seq., hereinafter referred to collectively as "the Plan(s)."

WHEREAS, PEIA is a Covered Entity as defined by 45 CFR §160.103 of The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (PUBLIC LAW 104-191).

WHEREAS, the PEIA Director is charged with identifying and implementing programs designed to promote the health and well-being of Plan covered members and dependents, and is permitted to contract for such services or programs that provide services to beneficiaries, are appropriate in care, and will be provided at an efficient cost.

WHEREAS, Vendor is a properly licensed, registered, insured, and competent service provider performing the programs and services outlined in this Agreement.

WHEREAS, the Vendor is performing an administrative and/or service level function on behalf of the Covered Entity as it relates to the treatment and healthcare operations of the Covered Entity.

WHEREAS, Vendor desires to accept the terms and conditions herein, as it relates to services performed and payment for services rendered to beneficiaries of the Plan.

NOW, THEREFORE, in consideration of these Recitals and the mutual promises contained herein below, the Parties agree as follows:

Definitions

1. **Agreement.** This Agreement between PEIA and the Vendor, and any amendments thereof made in accordance with this Agreement, including any response(s) to any Request(s) for Proposal(s) (RFPs) where language is incorporated by reference.

2. **Breach.** As defined in 45 CFR §164.402, a HIPAA breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

3. **Business Associate.** Any entity as defined by 45 CFR Parts 164.502(e), 164.504(e), 164.532(d) and (e) who performs a service on behalf of a Covered Entity.

4. **Business Associate Agreement.** The State of West Virginia Executive Branch Business Associate Agreement which is hereby incorporated by reference as part of this Agreement.

5. **Covered Person.** Any individual person eligible for benefits under the Plan.

6. **NIST.** National Institute of Standards and Technology.

7. **PEIA.** The West Virginia Public Employees Insurance Agency, an agency of and for the State of West Virginia under the Department of Administration.

8. **PHI.** Protected Heath Information as defined by HIPAA.

9. **PII.** Personally Identifiable Information.

10. **RFP.** Request for Proposal whose terms and conditions are hereby incorporated by reference into this Agreement.

11. **Vendor.** The party, entity, and/or agent(s) being contracted with and/or being paid by PEIA for the product(s) and/or service(s) outlined in the Scope of Work section of the RFP that they responded to and/or the terms and conditions of this Agreement including, but not limited to: any employee(s) and/or agent(s) of the Vendor; any and/or all subcontractors and/or subcontractors of subcontractors of the Vendor; any and/or all collaborator(s) with and/or of the Vendor; or any other third party not a direct signature party to this Agreement who may be involved in the performance of the Scope of Work on this Agreement. If any conflict or inconsistency arises between the language of this Agreement and any Statement of Work, the RFP response and the terms of this Agreement shall control.

General Terms and Conditions

1. This Agreement shall be governed by the laws of the State of West Virginia regardless of the sites or locations of the Vendor and its contractors or subcontractors.

2. Vendor is in good standing under the laws, rules, and/or regulations of the State of West Virginia, and is duly licensed, registered, authorized and empowered to do business in the State of West Virginia as contemplated by this Agreement, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, the West Virginia Insurance Commission, or any other state agency or political subdivision, as applicable. Vendor shall maintain such authorization at its own cost. Vendor's failure to maintain such authorization shall be sufficient cause for termination of this Agreement. Vendor shall maintain active Purchasing registration with the State of West Virginia through the Vendor Self Service portal available and viewable at https://prd311.wvoasis.gov/PRDVSS1X1/Advantage4. Upon request, the

Vendor must provide all necessary releases to obtain information to enable the Agency to verify that the Vendor is licensed and in good standing with any applicable entities.

3. The Vendor agrees and understands that it is a contractor to PEIA and that no employer/employee relationship is created, either expressed or implied, by this Agreement.

4. The terms and conditions of the RFP response by the vendor are hereby incorporated by reference into this Master Services Agreement. PEIA may, at its own discretion, engage in a solicitation to seek competitive bids for the product(s) and/or service(s) being provided under this Agreement.

5. If this is a “proof of concept” Agreement whereby the Vendor, through its products and/or services, is responsible for demonstrating the improved standards of care, clinical efficacy, cost savings, and/or other benefits to the Plan and covered persons. The Vendor recognizes and acknowledges that PEIA reserves the right to go out to bid or otherwise seek to procure the same or similar services from other vendors.

6. The term of this Agreement shall be one (1) year commencing on the effective date, which shall be the last date upon which the Parties executed this Agreement.

7. Either party may terminate this Agreement, without cause, by giving thirty (30) days written notice to the other party.

8. This Agreement may be terminated upon thirty (30) days written notice by either party for any material breach by the other party. For purposes of this Agreement, the term "breach" shall mean and be specifically limited to the failure by either party to keep, observe or perform any covenant, agreement, term, covenant, or provision of this Agreement kept, observed or performed by such party, and the continuance of such breach for a period of thirty (30) days after notice thereof from the non-breaching party to the breaching party.

9. Except as otherwise provided herein, amendments, extensions or renewals of this Agreement shall be made in writing and executed by both Parties.

10. The waiver by either party of any breach or violation of any provision of this Agreement shall not operate as, or be construed to be, a waiver of any subsequent breach of the same or other provision hereof.

11. The following documents and their respective terms and conditions are hereby incorporated by reference into this Agreement:

    a. State of West Virginia WV-96 Purchasing Agreement Addendum

    b. State of West Virginia Executive Branch Business Associate Agreement and corresponding Appendix A

    c. State of West Virginia Data Exchange – Data Management Addendum

    The language of these documents shall supersede all terms and conditions to the contrary, either expressed or implied, in this Agreement.

12. The Vendor may not reassign the terms and conditions of this Agreement to any third party nor reassign its liability, roles and responsibilities for the performance of the Scope of Work of this Agreement to any third party without the express written permission of PEIA.

13. The pricing set forth in the Scope of Work herein is firm for the life of the Agreement, unless specified elsewhere within this Agreement.

14. Payment in advance is prohibited under this Agreement. Payment may only be made after services have been rendered. The Vendor shall submit invoices in arrears.

15. The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Agreement and the transactions contemplated thereby. PEIA is exempt from federal and state taxes and will not pay or reimburse such taxes.

16. Vendor agrees and understands that it is their responsibility to provide the product(s) and/or service(s) in the timeframe(s) and/or schedule for deliverables outlined in the then-current Scope of Work between the Parties. Failure to adhere to defined timelines and/or deliverable schedule(s) shall be grounds for termination of this Agreement.

Confidentiality

The Parties shall maintain this Agreement and the compensation arrangements agreed to herein in the strictest confidence and shall not disclose them to any person except as required by law and to further the purposes of this Agreement. Notwithstanding the foregoing, this Agreement may be subject to release or disclosure under applicable provisions of the West Virginia Freedom of Information Act ("FOIA") under West Virginia Code §29B-1-1, et. seq. should such a request be filed with PEIA. PEIA shall promptly notify Vendor of any FOIA request relating to this Agreement. It shall be the sole responsibility of the Vendor to defend against any release of information it deems to be confidential, proprietary, and/or a trade secret and/or otherwise protected from further disclosure under the applicable provisions of West Virginia Code §29B-1-1, et. seq.

Work Product – Ownership of Data

For all services provided by the Vendor, the concept of work product shall apply. Such concept shall mean and intend that all data provided, shared, gathered, garnered or obtained, and the results of all work performed with said data, shall be the sole property of PEIA with no rights of ownership, expressed or implied, conveyed to the Vendor. PEIA data may not be used, either in identified or de-identified format, for any purpose other than for the performance of the scope of work outlined in this Agreement.

Data Exchange

For purposes of the Scope of Work on this Agreement, only the minimum necessary Covered Persons' data will be disclosed to the Vendor for the meaningful use of performing the tasks, duties, or services outlined in this Agreement. The data may be provided in an identified or de-identified format, depending on the services outlined in the then-current Scope of Work between the Parties. PEIA reserves the right to limit the data elements in keeping with accepted minimum

necessary guidance. PEIA shall transmit the data to the Vendor in a secure and encrypted format in compliance with all applicable provisions of the HIPAA Security Rules.

Compliance

A. Vendor agrees to be compliant with all any and/or all applicable provisions of the following:

    1. The Genetic Information Non-discrimination Act of 2008 (GINA) - (Pub.L. 110–233, 122 Stat. 881, enacted May 21, 2008

    2. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (PUBLIC LAW 104-191) including both the Privacy and Security Rule(s) of HIPAA

    3. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009

    4. The Privacy Act of 1974, as amended, 5 U.S.C. § 552a

    5. NIST Guidance referenced in and as applicable to compliance with the above referenced law, e.g. NIST SP 800-53; NIST SP 800-66; NIST 800-88

B. Further, Vendor agrees to full compliance with the State of West Virginia Executive Branch Business Associate Agreement (WV BAA) and corresponding Appendix A as incorporated by reference into this Agreement. Vendor shall be responsible for ensuring that all subcontractors performing any of the scope of work related to this Agreement are informed of the terms and conditions of the WV BAA and agree to compliance thereto.

Subcontractors

The Vendor agrees to provide PEIA with the names of any and/or all subcontractors and/or collaborators who may perform any portion of the Scope of Work on this Agreement and/or who may have access to PEIA member PII/PHI. Further, the Vendor agrees to accept responsibility and liability for the actions, errors, and performance of any subcontractors who perform any portion of the scope of work on this Agreement. The Vendor shall be responsible for ensuring that any and/or all subcontractors and/or collaborators have been made aware of and are in compliance with the terms and conditions of this Agreement and the documents incorporated by reference into this Agreement.

Insurance

Vendor shall procure and maintain, at its sole cost and expense, policies of comprehensive general liability and other insurance in the minimum amounts of $1,000,000 per occurrence/$2,000,000 aggregate to insure such party and its officers, agents, and employees against liability, claims or damages in connection with the performance its responsibilities under this Agreement, and shall provide copies of such policies to PEIA. Said insurance shall include, at a minimum, coverage of $1,000,000 per occurrence/$2,000,000 aggregate, data breach/cyber breach liability insurance naming PEIA as a co-insured on said policy as it relates to the scope of work on this Agreement.

Legal Defense

PEIA shall have no obligation to defend the Vendor, or any subcontractors of the Vendor, in any legal action instituted on a claim of malpractice relating to Vendor services provided through this Agreement.

Data Disposition

Within sixty (60) days of the termination of this Agreement the Vendor shall provide to PEIA a detailed data disposition plan compliant with the applicable provisions of the HIPAA Security Rules that renders any and all PEIA data received, created, transmitted, stored, or otherwise maintained by Vendor unreadable, indecipherable, and/or otherwise unusable. This term and condition would also apply to any data held or stored by any subcontractor(s) and/or collaborators. Such plan shall outline the means and modes of data disposition and the means and modes of verifying or validating the proper disposition of the data.

Data Security Requirements

Vendor shall implement reasonable administrative, physical, and technical safeguards and/or restrictions regarding physical and electronic access to PEIA data, including but not limited to the following

I. Vendor Information Security Program

a. Physical access controls, secure user authentication protocols, secure access control methods, firewall protection, malware protection, and use of encryption for laptops, mobile devices and PEIA Data being transmitted across the public Internet or wirelessly, and as otherwise required by applicable law.
b. To the extent it does not already employ one, Vendor shall develop and maintain a reasonable and appropriate written data security policy that includes technological, physical, administrative and procedural controls to protect the confidentiality, integrity and availability of PEIA Data that encompasses access, retention and transport of PEIA Data, and that provides for disciplinary action in the event of its violation;
c. Vendor shall prevent terminated employees from accessing PEIA Data by immediately terminating their physical and electronic access to such PEIA Data;
d. Vendor shall employ assessment, monitoring and auditing procedures to ensure internal compliance with these safeguards;
e. Vendor shall conduct a complete assessment of these safeguards at least annually and, upon written request, provide a report on the results of the assessment, including but not limited to any discrepancies, to PEIA.
f. Vendor must have system hardening standards such that default configurations and deployments are appropriately modified to protect PEIA data.

II. Access Management and Authentication

a. The addition, deletion, and modification of user access must be formally defined processes, restricted to appropriate personnel, and must generate and retain an audit trail of applied changes.
b. Vendor must remove access for any terminated employees and any third party that no longer require access.

c. Vendor must employ least privilege user access.
d. User identity must be verified before performing any password reset.
e. Vendor must employ enhanced protections for privileged administration accounts
f. Industry best practices and security controls must be used throughout any Single Sign On and federated identity connections.
g. Passwords, including temporary passwords, must be systematically required to be strong and complex.
h. Passwords must be restricted from reuse.
i. Login and password change mechanisms must be protected against attack including account lockouts, throttling, activity logging and alerting or other effective protections.
j. Passwords should be stored using a strong password hashing function.
k. Vendor users with remote access to PEIA Data are required to use two-factor authentication.

III. Data Management

a. Vendor shall store PEIA Data in a manner allowing its identification, access, and destruction without inadvertently affecting or including another customer's data.
b. At termination of the Agreement, Vendor must provide a certificate of destruction of PEIA data.
c. No PEIA owned data shall be stored, used, transmitted, and/or otherwise accessed from any location outside the United States.

IV. Logging and Monitoring

a. Event logging must be in place for network, system, and application access. Logging must also be in place for access to secured physical location.
b. Logging should collect sufficient information to monitor an event including event type, timestamp, user origin, destination resource, and activity
c. Logs must be retained for a minimum of two hundred seventy (270) days and must be backed up in case of accidental deletion or corruption
d. Access to logs must be restricted to select administrators who have a business need to access.

V. Anti-virus Protection

a. Anti-malware software standards such that any equipment that transmits, receives, stores or processes PEIA Data has current anti-virus software and signatures installed

VI. Security Patching Management

a. Patch management standards must be in place to ensure that all infrastructure devices, operating systems and software are updated regularly, and updates are expedited when deemed critical. All new systems and devices must be configured with current security updates/patches and hardened before being put into production.

VII. Application Development

a. Industry best practices and security controls must be used throughout the software development life cycle (SDLC) for any development necessary to work with PEIA Data. Vendor must have a formal and documented SDLC policy that outlines release/development methodology as well as appropriate segregation of duties.
b. The SDLC must consider sufficient security testing of code at the unit, integrated, and production phases.
c. Vendor must maintain a formal change management process that includes segregation of duties between roles implementing and approving changes.
d. For internally developed applications (including web or mobile applications), there must be processes in place to control, monitor, and log developers' access and changes to the production environment.
e. Vendor must not use software with known high-risk vulnerabilities in any Vendor applications or services. All software components used in the application must be versions currently supported by the respective software vendors.
f. There should be separate development, test, and production environments.
g. Applications are to be scanned for vulnerabilities using effective tools or competent third parties.
h. Production data is not to be used for development, sales, marketing, and/or any other purposes not specifically outlined in this Agreement.

Physical Security

a. Physical security standards shall be in place to protect information from unauthorized physical and electronic access. Physical security standards, at a minimum, should be in accordance with relevant NIST Guidance found in and as applicable to compliance with the above referenced law, e.g. NIST SP 800-53; NIST SP 800-66; NIST 800-88
b. Vendor shall be able to provide upon request documentation of its administrative, procedural, and technical safeguards designed and intended to meet the Physical Security requirements of the HIPAA Security Rule(s).
c. Under no circumstance is any PEIA and/or State data, either in identified or a deidentified format(s), allowed to be transmitted, stored, used, viewed, and/or otherwise accessed outside of the forty-eight (48) contiguous states of the United States.

Personnel Security

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations, and ethics and should be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

Business Continuity

Vendor must have Business Continuation, Disaster Recovery, and Data Restoration plans in place that are updated and tested on at least an annual basis.

Security Training

Vendor must have a program in place to ensure employees and subcontractors are periodically trained on information security principles and failure to comply will be addressed through appropriate discipline imposed by Vendor or its subcontractors, as applicable.

Security Incident Response Procedures.

If Vendor (or Vendor's personnel, including contractors and/or subcontractors) discovers or suspects that an unauthorized access, use, copying, alteration, transfer, or other violation, compromise, breach or attempted breach of security (electronic or physical) involving or related to PEIA Data within its (or its personnel's) possession or control has occurred, whether the incident originates within Vendor's organization or externally (**"Security Incident"**), Vendor shall:

(a) immediately conduct a reasonable investigation of the reasons for and circumstances surrounding such Security Incident or reasonably suspected Security Incident;

(b) use best efforts and take all necessary actions to prevent, contain, and mitigate the impact of such Security Incident or reasonably suspected Security Incident;

(c) provide notice to PEIA at PEIAPrivacy@wv.gov within twelve (12) hours after the Vendor discovers or reasonably suspects a Security Incident;

(d) promptly, and in no event more than two (2) business days after the date Vendor discovers or reasonably suspects a Security Incident, provide a written report to PEIA concerning such Security Incident or reasonably suspected Security Incident;

(e) collect and preserve all evidence concerning the discovery, cause, vulnerability, remedial actions, and impact related to such Security Incident or reasonably suspected a Security Incident, which shall meet reasonable expectations of forensic admissibility;

(f) document the incident response and remedial actions taken in detail, which shall meet reasonable expectations of forensic admissibility;

(g) retain a qualified contractor to conduct a security assessment to determine whether Vendor was compliant with Applicable Law at the time of the Security Incident; and

(i) if requested by PEIA, provide notice to individuals or entities whose PEIA Data was or may have been affected, in a manner and format specified by PEIA.

(ii) Security Incident Status Reports. If PEIA is notified of any Security Incident or reasonably suspected Security Incident, or otherwise discovers or suspects that Vendor has suffered a Security Incident, upon PEIA's request Vendor shall provide PEIA with:

(a) a written status report concerning such Security Incident or reasonably suspected Security Incident; and

(b) any documents requested by PEIA related to such Security Incident or reasonably suspected Security Incident, including without limitation, any security assessment and security control audit reports, logs, and any forensic analysis of such Security Incident or reasonably suspected Security Incident.

(iii) Security Incident Information. In addition to any other information requested by PEIA, such written report as required in Section (**x)** shall include the following:

(a) the amount or number of records and type of PEIA Data reasonably suspected as having been accessed, compromised or misused;

(b) a list identifying the individuals or entities whose PEIA Data is at issue, including with respect to individuals, the name, address, phone number, and e-mail address of such individuals;

(c) a description of any wrongdoing or harm caused by the actual or reasonably suspected Security Incident, including without limitation, identity theft;

(d) a description of the Security Incident or reasonably suspected Security Incident, including without limitation, the findings of Vendor's investigation, the cause and timeframe of such Security Incident, the source of such Security Incident, and the vulnerability that led to the Security Incident;

(e) the remedial actions taken to date by Vendor and the results of such remedial actions; and

(f) the remedial actions planned by Vendor going forward and the timeframe for completing such remedial actions.

(iv) Preservation, Return, and Destruction of Documents. Vendor shall preserve information in accordance with PEIA's instructions and requests, including without limitation any retention schedules and litigation hold instructions provided by PEIA to Vendor, independent of where the information is stored (specifically, and without limitation, even where such information resides with or is held, processed or stored by a sub-contractor, vendor, or other third party). Vendor shall take reasonable steps to ensure proper destruction (such that information is rendered unusable and unreadable) and return of information to PEIA in a format requested by PEIA and at Vendor's expense when it is no longer needed to perform services pursuant to the Agreement or thirty (30) days following termination of the Agreement. Vendor shall provide written certification that all such information has been returned and deleted.

(v) Control and Access. Vendor shall cooperate with PEIA in responding to any party, non-party, or government request for information. In the event that such requests are served on PEIA, Vendor shall provide PEIA with access to such information in the format in which it is maintained in the ordinary course of business (or, on PEIA's request, with copies) within twelve (12) hours of receipt of any request by PEIA for such access or copies. In the event that such a request (in the form of a subpoena, order or otherwise) is provided to or served on Vendor, Vendor shall notify PEIA in writing by electronic mail to PEIAPrivacy@wv.gov immediately and in no event more than twenty-four (24) hours after receiving the request, subpoena, or order. Such notification must include a copy of the request, subpoena, or court order. Vendor also shall immediately inform in writing the third party who caused the request, subpoena, or order to issue or be provided or served on Vendor that some or all the material covered by the request, subpoena, or order is the subject of a nondisclosure agreement. Vendor shall cooperate with PEIA in seeking any protection from disclosure for such information that PEIA shall deem appropriate.

(vi) Document Authentication. In the event that PEIA is required to authenticate any document or information, Vendor shall cooperate with PEIA in providing any requested assistance with such authentication, including without limitation testifying (by affidavit, declaration, deposition, in court, or otherwise) as a custodian of records to authenticate the information, establish chain of custody, and provide any other requested information or assistance.

(vii) Indemnification.

(a) In addition to any indemnification obligations contained in other parts of the Agreement, Vendor agrees to indemnify, defend, and hold harmless PEIA and its affiliates, subsidiaries, successors, and assigns (and the officers, directors, employees, sublicensees, clients, and agents of PEIA, and its affiliates, subsidiaries, successors, and assigns) from and against any and all claims, losses, demands, liabilities, damages, settlements, expenses, and costs (including without limitation attorneys' fees and costs), and any and all threatened claims, losses, demands, liabilities, damages, settlements, expenses, and costs alleged, sustained or incurred by a third party, arising from, in connection with, or based on allegations of, any Security Incident or reasonably suspected Security Incident, any breach of the Data Security Requirements of this Agreement by Vendor, any failure of Vendor to comply with Applicable Law, including without limitation:

i. expenses incurred to provide warning or notice to PEIA's clients and employees, law-enforcement agencies, regulatory bodies, or other third parties;
ii. expenses incurred to investigate, assess, or remediate a Security Incident, reasonably suspected Security Incident, or failure to comply with any Applicable Law;
iii. expenses incurred to hire any public relations consultants to respond to a Security Incident or reasonably suspected Security Incident;
iv. expenses incurred to provide credit monitoring services to individuals affected by a Security Incident or reasonably suspected Security Incident;
v. expenses incurred to retain a call center to respond to inquiries regarding a Security Incident or reasonably suspected Security Incident;
vi. fines, penalties, or recovery amounts; and
vii. expenses incurred to respond or address any investigation by law-enforcement agencies, regulatory bodies, or other third parties.

(b) PEIA shall notify Vendor promptly of any claims or demands made by a third party against, or losses, demands, liabilities, damages, settlements, expenses, and costs incurred by, PEIA for which indemnification is sought; provided, however, that the failure to give such notice shall not relieve Vendor of its obligations under this Agreement except to the extent that Vendor was actually and materially prejudiced by such failure. PEIA may, at its option and expense, participate and appear on an equal footing with Vendor in the defense of any claim that is conducted by Vendor as set forth in in this Agreement. Vendor may not settle any claim without the prior written approval of PEIA. From the date of written notice from PEIA to Vendor of any such claim, PEIA shall have the right to withhold from any payments due Vendor under this Agreement the amount of any defense costs, plus additional reasonable amounts as security for Vendor's obligations under the Insurance Section of this Agreement.

(viii) Cooperation and Coordination. Vendor agrees to reasonably cooperate and coordinate with PEIA concerning:

(a) PEIA's investigation, enforcement, monitoring, document preparation, notification requirements, and reporting concerning Security Incidents, reasonably suspected Security Incidents, and Vendor's and PEIA's compliance with applicable law; and

(b) any other activities or duties set forth under this Agreement for which cooperation between PEIA and Vendor may be reasonably required.
(c) Any investigation and/or inquiry by an authority having jurisdiction in matters related to the enforcement of any state and/or federal privacy and/or security law(s), rule(s) and/or regulation(s), e.g. the U.S. D.H.H.S. Office of Civil Rights and/or the State of West Virginia Executive Branch Privacy Office.

(ix) Vendor's Expense. Vendor's compliance with Data Security Compliance Section of this Agreement and any actions required of Vendor by the Data Security Compliance Section of the Agreement shall be at Vendor's sole and exclusive expense and shall be included as part of the price of the services provided by Vendor for no additional fee, including without limitation, any PEIA requests authorized by Section (**x)** of the Agreement.

(x) Vendor Assurances. Nothing in this Agreement shall prohibit PEIA from performing or conducting additional vendor assurance reviews and/or audits designed and intended to ensure vendor compliance with applicable provisions of the HIPAA Security Rule(s).

Force Majeure

Neither party shall be liable or deemed to be in default for any delay or failure to perform under this Agreement which results, directly or indirectly, from acts of God, civil or military authority, acts of public enemy, war, accidents, fires, explosions, earthquake, flood, failure of transportation, strikes, pandemics or other work interruptions by either party's employees or any other cause beyond the reasonable control of either party.

Notice

Any notice, demand or communication which are, or may be, required, permitted, or desired by any party given to the other in connection with this Agreement, shall be in writing and shall be deemed to have been properly given when delivered personally or when sent by certified mail, return receipt requested, addressed as follows:

If to PEIA: Brent Wolfingbarger, Director
West Virginia Public Employees Insurance Agency
601 57th Street, SE
Charleston, West Virginia 25304
brent.wolfingbarger@wv.gov
Cc: william.b.hicks@wv.gov

If to Vendor: _____
_____
_____
_____

or to such other address, and to the attention of such other person or officer as the receiving party may designate, with copies thereof to the respective counsel thereof as designated by such party.

Agreement

This Agreement and any attachments, addenda or exhibits, including the State of West Virginia WV-96 Agreement Addendum which are incorporated herein by reference, constitute the entire agreement between the Parties relating to the subject matter of this Agreement. No party shall be entitled to benefits other than those specified herein. Together they supersede all previous contracts and all prior representations or agreements between the Parties, whether written or oral, pertaining to the subject matter of this Agreement. No changes in or additions to this Agreement shall be of any effect unless and until made in writing and signed by both Parties.

Rosters

Vendor agrees that PEIA, the State of West Virginia, or its designees may use Vendor's name, address, and other information in rosters of participating providers and marketing materials.

Scope of Work

The Vendor agrees and understands that PEIA shall not be responsible for any cost(s), fee(s), charge(s), and/or other liabilities not expressly defined in the Scope of Work between the Parties. Terms such as, “plus expenses”, “plus travel”, and/or any other non-fixed and/or undetermined shall be non-applicable to this Agreement.

For issues with regard to payment for product(s) and/or service(s), please refer to the State of West Virginia WV-96 Form incorporated by reference into this Agreement.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed in multiple originals by their duly authorized officers.

Vendor	PEIA
By: _____	By:_____
Its:_____	Its:_____
Date:_____	Date:_____

Attachment 12
SUBCONTRACTOR INFORMATION FORM

Name	
Address	
Contact Person	
Description of Work to be Subcontracted	
Descriptive information concerning organizational abilities	

Name	
Address	
Contact Person	
Description of Work to be Subcontracted	
Descriptive information concerning organizational abilities	

Attachment 13
VENDOR EXPERIENCE FORM

Contact Person	
Position	
Address	
City, State, Zip	
Telephone Number	
E-mail Address	
Project Description	
Number of Lives	
Project Dates	
Personnel Assigned	

Attachment 14
STAFF RESUMES

Name	
Title	
Relevant Experience	
Relevant Certifications	
Education	

Name	
Title	
Relevant Experience	
Relevant Certifications	
Education	

Attachment 15
DEVIATIONS PAGE

Vendor MAY NOT request an exception, clarification, or modification to circumvent a mandatory minimum requirement. PEIA is under no obligation to consider or negotiate any of the proposed items.

ORIGINAL RFP ITEM & LOCATION	VENDOR PROPOSED EXCLUSION, CLARIFICATION, OR MODIFICATION

Attachment 16

ADDENDUM ACKNOWLEDGMENT FORM
SOLICITATION NO. ARFP PEI2700000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[ ] Addendum No. 1	[ ] Addendum No. 6
[ ] Addendum No. 2	[ ] Addendum No. 7
[ ] Addendum No. 3	[ ] Addendum No. 8
[ ] Addendum No. 4	[ ] Addendum No. 9
[ ] Addendum No. 5	[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

AUTHORIZED SIGNATURE	
COMPANY	DATE

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document proces

Attachment 17
ADDENDUM DETAIL - ADDENDUM 1

The purpose of this addendum is to modify the solicitatoin identified as [ARFP PEI2700000001] ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category

[**X**] Modify bid opening date and time
[ ] Modify specifications of product or service being sought
[ ] Attachment of vendor questions and responses
[ ] Attachment of pre-bid sign-in sheet
[ ] Correction of error
[**X**] Other

Description of Modification to Solicitation

1. Pushed back the PEIA Responses Deadline by one week from 10/16/26 to 10/23/26; thereby also pushing back the Bid Due Date by one week from 11/6/26 to 11/13/26.
2. Added Attachment 17 (Addendum Detail)
3. Added new Attachment to Section 10 list
4. Updated RFP Due Date on Attachment 2 (Cost Proposal)
5.
6.

Terms and Conditions

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect
2. Vendor shall acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith in the Terms and Conditions. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgment should be submitted with the bid to expedite.