REQUEST FOR QUOTATIONS
Third Party Administrator Consulting

ARFQPEI2100000001

West Virginia Public Employees Insurance Agency
601 57th Street, SE, Suite 2
Charleston, West Virginia 25304-2345
304-558-7850
Fax: 304-558-2470

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Public Employees Insurance Agency (PEIA) is seeking an experienced consultant to help design and administer a Request for Proposals (RFP) to obtain a Medicare-Advantage Prescription Drug (MAPD) plan for the Medicare primary retirees. PEIA is the State agency that is responsible for administering health care benefits to approximately 52,026 Medicare primary retirees and dependents for state, county, and municipal employees.

   1.1. PEIA has determined that it is necessary to bid the contract for all MAPD services. PEIA desires all bids to have separate pricing for: (1) TPA claims processing and management services for the Medicare primary retired members and their dependents; (2) An optional proposal to administer benefits for non-Medicare retirees and their dependents.

   1.2. The successful MAPD would assume not only responsibility for all medical and prescription claims of the above groups, but also a comprehensive list of other services, including but not limited to network management, utilization review, prior authorization, benefit design, identification cards and member communication, disease management, customer and client support, reporting, provider profiling, and other ancillary services.

   1.3. Due to the enormity and complexity of this contract award, PEIA desires to employ a consultant for development of the RFP, issuance of the RFP, and evaluation of the responses. The vendor will be the point of contact for the entire RFP development, issuance, bidder's conference, questions and answers, evaluation, and recommendation for award of the contract. PEIA will be involved in the entire process.

   1.4. The MAPD RFP must be released no later than December 1, 2020, with a successful vendor to be selected by March 15, 2021. The effective date of the MAPD contract to be awarded, will be the beginning of Plan Year 2022, which is effective January 1, 2022.

1.5. RFQ Schedule

RFQ Issued	July 29, 2020
Vendor Questions Due to PEIA	August 10, 2020, 4:00 p.m., ET
PEIA Responses to Vendor Questions	August 17, 2020,
Vendor Quotes Due to PEIA	August 28, 2020, 4:00 p.m., ET
PEIA Evaluation Period	August 28 through September 23, 2020
Notification to Successful Vendor	September 23, 2020
Contract Award	September 23, 2020

All communication, inquiries, and final quotations regarding this RFQ must be submitted in writing to the following individual:

Ms. Charlotte K. Stover, MS
Deputy Director of Insurance and Members Services
WV Public Employees Insurance Agency
601 57th Street, SE, Suite 2
Charleston, WV 25304-2345
Facsimile: (304) 558-2470
E-mail: Charlotte.K.Stover@wv.gov

2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

2.1 Business Associate describes an entity as defined by 45 CFR 160.103, 164.502(e), 164.504(e), and 164.532(d) and (e) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

2.2 "Contract Services" means the successful vendor consultant will provide PEIA with a potential Request for Proposal (RFP) consistent with the requirements listed in this solicitation.

2.3 Covered Entity means an entity as defined under 45 CFR 160.103.

2.4 HIPAA means the Health Insurance Portability and Accountability Act of 1996.

2.5 "Pricing Page" means the pages upon which Vendor should list its proposed price for the Contract Services. The Pricing Page is attached hereto as Exhibit A.

2.6 "RFQ" means the official Request for Quotations published by PEIA, identified as ARFQ PEI2100000001

2.7 "MAPD" means a Medicare Advantage Prescription Drug Plan as authorized and approved by CMS.

2.8 "Solicitation" means the official notice of an opportunity to supply the State with goods of services that is published by the Purchasing Division.

2.9 CMS means the United State Department of Health and Human Services Centers for Medicare and Medicaid Services.

2.10 "Vendor or Bidder" are used interchangeably throughout this solicitation.

2.11 "TPA" means third party administrator.

3. **QUALIFICATIONS:** The Bidder must demonstrate its ability to meet the following qualifications in order to submit a quotation. Failure to demonstrate the ability to meet these qualifications will automatically disqualify the Bidder. The Bidder must restate each question/item in the RFQ response then provide the response. The Bidder shall have the following minimum qualifications:

3.1. Minimum of five (5) years consulting experience related to health care and/or MAPD plans benefit management.

3.2. Minimum of five (5) years consulting experience with health care and/or MAPD plans with a minimum of 15,000 covered lives.

3.3. The Bidder should list any experience in consulting with State and/or local government sponsored health plans in detail.

3.4. The Bidder responding to this request must submit in writing a synopsis of experience completing relevant projects of plans with a minimum of 15,000 covered lives of similar scope and nature completed within the last 36 months.

3.5. The Bidder should be completely independent from, and not have any affiliations, partnership, or agreement with, any of the following including, but not limited to, Pharmacy Benefit Manager (PBM), Third Party Administrator (TPA), Medicare Advantage Plan (MAPD) mail order pharmacy services, drug manufacturing or distribution services. The Bidder must agree not to accept any commissions, service fees, finder fees, or any monetary remuneration from any potential vendor before or after the issuance of this resulting RFP.

3.6. The Bidder that prepares the RFP will be ineligible to submit a bid for the contract of any of the TPA services arising from this RFP.

3.7. If you are submitting a proposal to this RFQ and there are relationships with any potential conflicts of interest, the Bidder must provide full disclosure.

3.8. PEIA is a Covered Entity as defined by 45 CFR 160.103. The Bidder, in performing an Administrative function on behalf of the Covered Entity, would be considered a Business Associate as defined by 45 CFR 160.103, 164.502(e), 164.504(e), and 164.532(d) and (e) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and, as such, would be required to sign the West Virginia Executive Branch Business Associate Agreement, Exhibit B, with corresponding Appendix A.

3.9. The successful Bidder must be or become a registered vendor in the State of West Virginia prior to the contract award in order to be awarded a contract. For more information regarding becoming a registered vendor, please visit: http://www.state.wv.us/admin/purchase/VendorReg.html.

3.10. The Bidder must provide three (3) references from previous customers that have utilized the Bidder to consult on a project of similar scope, including the writing and evaluation of an RFP, Your response must include the client name, address, contact person, email address, and telephone number.

3.11. This bid is not being accomplished through the State Purchasing Division. However, basic State Purchasing concepts will apply. The Bidder providing the quotes should generally comply with state contracting requirements outlined at: http://www.state.wv.us/admin/purchase/handbook/2007R24/default.html.

3.12. The bidder must disclose any real and/or potential conflicts of interest in regard to this solicitation as it relates to the proposed scope of work.

3.13. The Bidder must complete the attachments and forms in all links in this RFQ. Failure to complete in its entirety will result in disqualification.

3.14. The bid proposal will be awarded on a fixed fee contract basis. **See Exhibit A – Pricing Page**.

4. MANDATORY REQUIREMENTS:

4.1 Mandatory Contract Services Requirements and Deliverables: Contract Services must meet or exceed the mandatory requirements listed below.

4.1.1 By submitting a quote in response to this solicitation, the Vendor must agree to all of the terms and conditions of the West Virginia Purchasing Agreement Form WV-96 found here:

https://www.wvhepc.org/resources/RFB-RFP/RFP_17146_CTCS_Website/Exhibit_C.pdf

4.1.2 By submitting a quote in response to this solicitation, the Vendor must agree to sign the West Virginia State Government HIPAA Business Associate Agreement Addendum attached to this RFQ and viewable at: http://www.state.wv.us/admin/purchase/vrc/WvBaaAgEffectiveJun2013.pdf.

4.1.3 PEIA will provide the following to the successful vendor:

4.1.3.1 A list of potential bidders to be developed with the Consultant.

4.1.3.2 Background information, data, current challenges, PEIA objectives, and any census-type data necessary for inclusion in the RFP.

4.1.3.3 PEIA mandatory criteria/terms.

4.1.3.4 Mandatory contract terms for the successful vendor.

4.1.3.5 Mandatory forms for inclusion in this RFQ:

4.1.3.5.1 http://www.state.wv.us/admin/purchase/vrc/wv96.pdf.

4.1.3.5.2 http://www.state.wv.us/admin/purchase/vrc/WvBaaAgEffectiveJun2013.pdf.

4.1.4 The Consultant vendor shall provide:

4.1.4.1 Industry expertise in the development, issuance, and analysis of an MAPD RFP.

4.1.4.2 Analysis must include:

4.1.4.2.1 Network disruption

4.1.4.2.2 Pharmacy/Drug disruption

4.1.4.2.3 Star Ratings across national and local networks and how it impacts pricing.

4.1.4.3 Instructions to potential vendors including, but not limited, to proposal submission form and style; services to be expected; financial viability; network/provider availability; claims processing procedures; utilization management protocols; disease

management services; benefit design, customer service, and all other services related to PEIA's MAPD.

4.1.4.4 Develop the RFP in a manner that would allow the vendors to bid separate services or all services being requested by PEIA. Bids must include a base price with optional products such as dental and vision priced separately.

4.1.4.5 Detailed questions and tables to be included to determine the proficiency and experience of the vendor(s) in the areas for which the vendor is bidding. The questionnaire will include at a minimum any financial arrangements, system interfaces and technical requirement, claim administration services, customer service metrics, general vendor history, legal and liability conditions, references, reporting and performance guarantees.

4.1.4.6 Detailed design of a cost proposal that will allow a concise and equitable comparison of all RFP bidders' services in either part or as a whole service provider.

4.1.4.7 Ability to perform a full network evaluation and cost analysis to compare potential carriers.

4.1.4.8 Proposal requirements to include administrative reporting and claim management needs specific to PEIA and any additional costs that may be associated with ad hoc reporting requirements.

4.1.4.9 Measurement criteria that will be used to select the carrier or finalists.

4.1.4.10 A list of potential bidders to be developed with PEIA.

4.1.4.11 Act as a liaison for data exchanges necessary for TPA bidders to receive data needed for the submission of qualified and competent proposals.

4.1.4.12 A detailed written comparison of the evaluations of the RFPs submitted by the bidders with analysis and recommendations,

including a comparative analysis of the top three recommendations.

4.1.4.13 Availability and support in defense of a contract award in the event of an administrative or legal challenge to the contract award to explain the evaluation process.

4.1.4.14 Availability and participation in the Bidder's Conference and in preparing responses to questions.

4.1.5 Mandatory Legal Requirements

4.1.5.1 This RFQ and all work performed under the scope of work of any resulting Agreement shall be governed by the laws of the State of West Virginia.

4.1.5.2 PEIA is a Covered Entity as defined by 45 CFR 160.103. The Bidder, in performing an Administrative function on behalf of the Covered Entity, would be considered a Business Associate as defined by 45 CFR 160.103, 164.502(e), 164.504(e), and 164.532(d) and (e) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and, as such, would be required to sign the West Virginia Executive Branch Business Associate Agreement. The Business Associate Agreement shall be communicated to any and/or all subcontractors who may perform any of the Scope of Work on this procurement. The Appendix A for the Business Associate Agreement will be completed with the successful Bidder(s).

4.1.5.3 The Bidder(s) must identify any and/or all subcontractors who will or may perform any of the Scope of Work on this procurement including name(s) and contact person(s) in their response to this RFQ.

4.1.5.5 Any and/or all current PEIA MAPD contract terms, reimbursement/network information, and/or other existing MAPD information shared by the PEIA to or with the Bidder(s) shall be considered confidential, proprietary, and/or otherwise not subject to any further disclosure and/or release. Such information shall be considered the sole property of the State of West Virginia and shall

not be subject to release and/or further disclosure(s) under the Freedom of Information Ader the Freedom of Information Act as defined by WV Code §29B-1.

4.1.5.6 This RFQ , any bid proposals, and any resulting contract is subject to public disclosure under the West Virginia Freedom of Information Act ("FOIA"). Accordingly, if the Bidder considers any part of its bid proposal to contain 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. See, W. Va. Code § 29B-1-4(a)(1) here: http://www.wvlegislature.gov/WVCODE/ChapterEntire.cfm?chap=29B&art=1&section=4#01. The bidder shall be solely responsible for the defense of their redacted proposal(s). PEIA assumes no liability for defending any release under FOIA. Should PEIA receive a FOIA request for production of the response(s) to this RFQ, the bidder's redacted copy will be provided to the requestor(s). If no redacted copy of a bid proposal is submitted, PEIA shall release the unredacted copy(ies) of the bid proposal(s).

4.1.5.7 By submitting a quote in response to this solicitation, the Vendor must agree to sign the West Virginia Data Exchange – Data Management Addendum attached to this RFQ.

4.1.5.8 By submitting a quote in response to this solicitation, the Vendor agrees and understands that any and/or all work performed on behalf of PEIA in relation to the scope of work outlined in the resulting agreement and/or contract shall be considered work product and is the sole property of PEIA and the State of West Virginia. Such work product is not subject to any further dissemination, release and/or disclosure without the express written permission of PEIA.

4.1.5.9 Anyone performing under this Contract will be subject to PEIA's and/or the State of West Virginia Executive Branch's security protocol and procedures.

4.1.5.10 By submitting a quote in response to this solicitation, the Vendor agrees and understands that it, as an corporation, entity or organization, shall be liable for any and/or all violation of the terms and conditions of sections 4.1.5.1 through 4.1.5.9 and referenced documents by any of its employees, agents, contractors, and/or subcontractors.

5. CONTRACT AWARD:

5.1 The Contract is intended to provide PEIA with a purchase price for the identified Contract Services. The intent of this RFQ is for the Contract to be awarded to the Vendor that provides the Contract Services meeting the required specifications for the lowest overall total cost as shown on the Pricing Page. PEIA reserves the right to reject any and/or all bids.

5.2 Pricing Page: Vendor should complete the Pricing Page by providing a fixed fee cost for all services outlined in this RFQ.

Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation. See Exhibit A of this RFQ.

6. **PERFORMANCE:** Vendor and PEIA shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by PEIA. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

7. **PAYMENT:** PEIA shall pay fixed fee contract, as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

8. **TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by PEIA separately.

9. **FACILITIES ACCESS:** Performance of Contract Services may require access cards and/or keys to gain entrance to PEIA's facilities. In the event that access cards and/or keys are required:

   9.1. Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.

   9.2. Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.

   9.3. Vendor shall notify PEIA immediately of any lost, stolen, or missing card or key.

   9.4. Anyone performing under this Contract will be subject to PEIA's security protocol and procedures.

   9.5. Vendor shall inform all staff of PEIA's security protocol and procedures.

10. VENDOR DEFAULT:

10.1. The following shall be considered a vendor default under this Contract.

10.1.1. Failure to perform Contract Services in accordance with the requirements contained herein.

10.1.2. Failure to comply with other specifications and requirements contained herein.

10.1.3. Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

10.1.4. Failure to remedy deficient performance upon request.

10.2. The following remedies shall be available to PEIA upon default.

10.2.1. Immediate cancellation of the Contract.

10.2.2. Immediate cancellation of one or more release orders issued under this Contract.

10.2.3. Any other remedies available in law or equity.

11. MISCELLANEOUS:

11.1. This Contract shall be governed by the laws of the State of West Virginia.

11.2. Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor must provide in writing its Contract manager and his/her contact information within its bid.

11.3 All communication, inquiries, and final quotations regarding this RFQ must be submitted in writing to the following individual:

Ms. Charlotte Stover, MS
Deputy Director of Insurance and Members Services
WV Public Employees Insurance Agency
601 57th Street, SE, Suite 2
Charleston, WV 25304-2345
Facsimile: (304) 558-2470
E-mail: Charlotte.K.Stover@wv.gov

The Vendor, or anyone on its behalf, is not permitted to make any contact whatsoever with any member of the evaluation committee. Violations may result in rejection of the bid.

The Vendor, or anyone on its behalf, is not permitted to make any contact whatsoever with any member of the evaluation committee. Violations may result in rejection of the bid.

Exhibit A

Pricing Page

Vendor Name: _____

Vendor Contact Information

Address: _____

Phone Number: _____

E-mail: _____

Development, issuance, and evaluation of an RFP
$

Payment will be made when the following milestones are met:

30% of total to develop RFP
40% of total to complete evaluation of RFP
30% of total upon award of the TPA contract

The signature below binds the Vendor to the pricing submitted for the scope of work to be performed under this RFQ.

Vendor Signature: _____

Title: _____

Date: _____

Exhibit B

West Virginia Executive Branch
HIPPA Business Associate Addendum

with corresponding Appendix A

Exhibit C

West Virginia Data Exchange – Data Management Addendum

Exhibit B

West Virginia Executive Branch
HIPPA Business Associate Addendum

with corresponding Appendix A

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:

Name of Agency: The West Virginia Public Employees Insurance Agency

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 this agreement this shall specifically include, but not be limited to:

(1) Prescription claim information, and
(2) Underlying medical treatment and diagnosis information

Specifically, the data to be released to the Associate will include, but not necessarily be limited to de-identified medical and/or pharmacy claims information needed for developing and distributing a Request for Proposals for Third Party Medical Claims Administration and/or Management. It shall be the responsibility of the Associate to inform PEIA of what specific data elements are needed in order to fulfill the scope under this Agreement. Accordingly, the following terms and/or conditions shall apply to this Business Associate Agreement and Addendum:

1) PEIA reserves the right to determine the method(s) for the de-identification of data to be released.
2) Only the minimum necessary data allowing for the vendor to perform the scope of work as defined in the Agreement shall be released from PEIA to the Associate.
3) Any and/or all data exchange(s) shall occur using secure data transfer through the PEIA FTP site(s).
4) The Associate agrees to comply with any and/or all applicable provisions of the Privacy and Security Rule(s) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including the Omnibus Security Rule and the Health Information Technology for Economic and Clinical Health Act (HITECH).
5) This Agreement may involve data sharing between PEIA, the Associate, and other Business Associates of PEIA.
6) The PHI covered by this DUA may not be used by the Associate for any purpose other than the proper management and administration of the scope of work administered by the Associate with regard to its Agreement with PEIA. No other use(s), release(s), and/or further disclosure(s) is/are permissible under this agreement. The Associate is expressively prohibited from using PEIA member data and/or PHI for any other contract(s), agreements, research projects, purposes, and/or service agreement(s) with any other entity other than PEIA.
7) The Associate will report to PEIA, in writing, any breach, unauthorized use or disclosure of the PHI not provided for by this Agreement of which it becomes aware with one (1) business day.
8) Upon completion of the scope of work of the Agreement, the Associate shall, at the direction of PEIA, dispose of the data provided to the Associate by PEIA in a mode, means, and/or manner consistent with the provision(s) of the Security Rule(s) of HIPAA
9) Nothing in this agreement shall convey ownership rights and/or privileges for the data shared by PEIA to the Associate. Ownership rights and privileges to the data covered in this Agreement shall solely reside with the West Virginia Public Employees Insurance Agency.
10) The interpretation of this Agreement shall be made under the law(s) of the State of West Virginia.

Exhibit C

West Virginia Data Exchange – Data Management Addendum

Data Exchange – Data Management Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN.

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.

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.

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 public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. 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

U.S. data centers. 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:

Name of Agency:_____ 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: _____