State of Delaware
Office of Management & Budget
Statewide Benefits Office

STATE EMPLOYEE BENEFITS COMMITTEE

Request for Proposal for the
State of Delaware's Vision Insurance Benefit Program

Addendum #1

June 8, 2016

OMB15001 – VisionIns

1. **Eligibility and Enrollment**

   Throughout the document where eligibility file(s) are referenced, the term should have been "enrollment file(s)". Specifically, Page 6, Section C – Scope of Work, paragraph (g); Page 24, #6; and Page 27, #32. When an eligibility file is produced, it is for all State employees (and retirees, if applicable) that may elect a benefit. For the vision insurance benefit, only the employees and retirees that have elected vision insurance coverage are provided to the vendor.

   A. In the Scope of Work, Pages 6 and 7:

       i. Paragraph (h) is deleted in its entirety and replaced with:

           Accepting enrollment files in existing file layouts.

       ii. Paragraph (l) is added as follows:

           Ease of access to a secure web portal by benefit representatives and Pension Office personnel for changes in enrollment due to events such as enrolling new hires and qualifying events.

   B. In the Minimum Requirements, Pages 27 and 28:

       i. Paragraph 25 is revised to delete the second sentence.

       ii. Paragraph 32 is revised to reference enrollment files and remove the phrase "payroll deduction files".

       iii. Paragraph 33 regarding a single-sign-on enrollment process is deleted in its entirety.

       iv. Paragraph 35 is revised to add the following sentence at the end of the paragraph: Refer to Question 25 regarding the State's self-invoice process.

   C. In the Questionnaire, *General Questions*, eligibility status refers to enrollment status. Specifically, Page 34, #12a. and Page 36, #26.

   D. In your bid response, *Performance Guarantees*, please replace "eligibility" with "enrollment" in all instances for the categories Eligibility Updating, Eligibility Reporting, and Eligibility Accuracy.

2. **File Layout**

   In Section V., *Technical Standards and Security Requirements*, paragraph #1, *File Layout* on page 39, is deleted and replaced in its entirety with the following paragraphs (a) and (b) as follows:

a. Please confirm that your organization will accept, process, and reconcile enrollment as follows:

The State of Delaware (PHRST) will provide an active employee enrollment file on a weekly basis and the Pension Office will provide a retiree enrollment file on a weekly basis. Enrollment changes to a member's information such as an address change must be processed by the vendor. Termination of an employee's or pensioner's coverage and their dependents, if any, must be processed by comparing the current enrollment file to the existing enrollment in the contractor's system. A weekly reporting of enrollment discrepancies will be reported back to the Statewide Benefits Office (PHRST file) and the Pension Office (Pension file).

Response:

b. Please confirm that your system will accept the file layouts, see Attachment 3. **Changes, either of a data type or addition of a data type, will not be accepted.** The vendor must use the current file specifications and will only receive the employee and pensioner identification numbers. Under no circumstances will the full nine (9) digits for social security numbers be released.

Response:

3. **Appendix S – Data Confidentiality Agreement**

Pages 85 and 86, *Data Confidentiality Agreement* is deleted and replaced in its entirety with "Data Confidentiality Agreement, Addendum #1 - Version 2", which are pages 5 – 13 herein.

4. **Minimum Requirements**

Please copy and paste the following revisions or additions as indicated:

A. Page 24, #6, is deleted in its entirety and replaced as follows:

Please confirm that enrollment information, such as a Welcome Packet, will be mailed to the homes of all newly enrolled employees or retirees within fourteen (14) calendar days upon receipt of the enrollment file from the State.

B. Page 24, #5, the phrase "new products" is replaced with "vision health".

C. Page 32, the following requirement is added as paragraph #70:

The State acknowledges that a contractor has the right to exercise full control over the employment direction, compensation and discharge of all persons employed by the contractor in the performance of services for their clients. However, please confirm that, if awarded the contract, your organization will attempt to honor the State's request for

specific individuals to be assigned to managerial roles in all areas of account management.

Response:

C. Page 32, the following requirement is added as paragraph #71:

Please confirm that, if awarded the contract, your organization will provide a written report no later than forty-five (45) days following the close of each quarter which shall describe any judgment or settlement or pending litigation involving Contractor that could result in judgments or settlements in excess of One Hundred Thousand Dollars ($100,000).

Response:

D. Page 32, the following requirement is added as paragraph #72:

Please confirm that your company complies with all federal, state and local laws applicable to its activities and obligations including:

a. the laws of the State of Delaware;

b. the applicable portion of the Federal Civil Rights Act of 1964;

c. the Equal Employment Opportunity Act and the regulations issued there under by the federal government;

d. a condition that the proposal submitted was independently arrived at, without collusion, under penalty of perjury; and

e. that programs, services, and activities provided to the general public under resulting contract conform with the Americans with Disabilities Act of 1990, and the regulations issued there under by the federal government.

If awarded the contract, your organization will keep itself fully informed of and shall observe and comply with all applicable existing Federal and State laws during its performance of the work. If your organization fails to comply with (a) through (e) of this paragraph, the State reserves the right to terminate the contract or consider the Contractor in default.

Response:

E. Page 29, #48, the last paragraph is deleted in its entirety and replaced with the following:

Please provide a copy of your certificate of insurance with the appropriate types and coverage levels. At this time, you must provide a copy of your certificate of insurance with the appropriate types and coverage levels, and, if awarded the contract, please

confirm your understanding that the vendor <u>must</u> provide a copy of your certificate of insurance before any work is done pursuant to the terms in the RFP and resulting contract.

(continued on the next page)

APPENDIX O

DATA CONFIDENTIALITY AGREEMENT

| Addendum #1, Version 2 |

Data Exchange for Enrollment Purposes for Vision Insurance Benefit Program

This Data Confidentiality Agreement ("Agreement") is undertaken and effective on the date of the State Employee Benefit Committee (SEBC") award on _____ pursuant to the parties' performance of a certain contract ("Contract") effective July 1, 2016, by and between the State of Delaware ("State") by and through the Office of Management and Budget ("OMB") on its own behalf and on behalf of the group health plan it sponsors for employees, retirees, and other covered persons, collectively referred to hereafter as "Covered Persons", and _____ ("Contractor") with offices at _____ _____, ("Parties").

WHEREAS, the State issued a Request for Proposal ("RFP") for the Vision Insurance Benefit Program on May 26, 2015;

WHEREAS, the State Employee Benefit Committee's ("SEBC") representatives on the Proposal Review Committee ("PRC") have voted to recommend the award of the Contract to the SEBC for the Contractor to administer the program as provided in the RFP;

WHEREAS, Contractor desires to provide such data technology services to the State on the terms set forth in the Request for Proposal and as stated below;

WHEREAS, in order to implement the election of this benefit for the Covered Persons, the State and Contractor must exchange test and enrollment files prior to the effective date of the Contract;

WHEREAS, the information exchanged by the Parties is classified as Personally Identifiable Information (PII) and is information that, if divulged, could compromise or endanger the people or assets of the State and is data that is specifically protected by law; and

WHEREAS, the State and Contractor represent and warrant that each party has full right, power and authority to enter into and perform under this Agreement;

FOR AND IN CONSIDERATION OF the premises and mutual agreements herein, the State and Contractor agree as follows:

1. The RFP provides for data extracts to be used for enrollment and discrepancy reporting by the Covered Persons in the Contractor's Vision Insurance benefit program. Said files will be provided to the Contractor by and through Payroll Human Resources Statewide Technology ("PHRST") for active employees and the Pension Office for retirees.

2. The RFP requires that the Contractor accept the enrollment files in specified formats.

3. In order to facilitate a Covered Person's voluntary election of the benefit on or after the effective date of the Contract, the data is to be used for the following purposes and is not to be used for any other purpose.

   a. To populate the Contractor's test environment; and

   b. To populate the Contractor's system so that the Covered Persons who voluntarily elect the benefit during the Open Enrollment term in May, 2016, may be enrolled by the Contractor for coverage beginning on July 1, 2016.

4. The test files provided will be a sampling of active employees and pensioners who may not elect coverage. Therefore, those files need to be destroyed. On or before August 31, 2016, Contractor shall dispose of the test files in its systems or otherwise in its possession or under its control and in all of its forms, for example: disk, CD/DVD, backup tapes, and paper. The data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and the attached certificate of destruction form shall be provided to the State of Delaware.

5. The enrollment files generated by PHRST and the Pension Office will be placed in a sub-folder on the State's SFTP server. The Contractor is responsible to obtain the files from the server.

6. No clause of this Agreement shall be considered a waiver of any portion of the terms set forth in the RFP for which a Contract has been awarded to the Contractor. The terms of the document entitled *Non-Public Data Owned by the State of Delaware – Mandatory Terms and Conditions*, which is part of the RFP and a copy of which is attached hereto for reference, shall apply to the test files, enrollment files, and premium payment reconciliation files that will be exchanged prior to the effective date of the Contract.

This Agreement was drafted with the joint participation of the undersigned Parties and shall be construed neither against nor in favor of either, but rather in accordance with the fair meaning thereof.

IN WITNESS THEREOF, the Parties hereto have caused this Agreement to be in effect as of the latest date and year below written.

STATE OF DELAWARE   **CONTRACTOR**
OFFICE OF MANAGEMENT AND BUDGET

_____   _____
Signature   Signature
Brenda L. Lakeman   Printed Name: _____
Director of HR Mgt and Benefits Administration   Title: _____

_____   _____
Date   Date

Attachment to
DATA CONFIDENTIALITY AGREEMENT

Non-Public Data Owned by the State of Delaware – Mandatory Terms and Conditions

1. **Data Ownership:** The State of Delaware shall own all right, title and interest in its data that is related to the services provided by this contract.**[1]** The Service Provider shall not access State of Delaware User accounts, or State of Delaware Data, except (i) in the course of data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State of Delaware's written request.

2. **Data Protection:** Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Service Provider to ensure that there is no inappropriate or unauthorized use of State of Delaware information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions:

   a) All information obtained by the Service Provider under this contract shall become and remain property of the State of Delaware.

   b) At no time shall any data or processes which either belongs to or are intended for the use of State of Delaware 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 State of Delaware.

3. **Data Location**: The Service Provider shall not store or transfer non-public State of Delaware data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of Delaware data remotely only as required to provide technical support.**[2]**

4. **Encryption:**

   a) **Data in Transit**: The Service Provider shall encrypt all non-public data in transit regardless of the transit mechanism. The policy documents are located at:

---

[1] If, due to the nature of your product, the ownership of the data transfers to your organization when the data is under your control, please so state and provide an explanation and, if applicable, a citation for a regulation or law.

[2] The awarded vendor will be required to comply with the Offshore IT Staffing Policy: http://dti.delaware.gov/pdfs/pp/OffshoreITStaffingPolicy.pdf. The primary contractor must reside in the United States, be licensed for business in Delaware, and shall be liable for any noncompliance by any subcontractor. It is explicitly forbidden for the primary contractor or subcontractor staff to "share" access privileges. Describe your organization's relationship with any offshore staff, either as employees of your company or that of any subcontractor. State the scope (number and location) of the personnel, their role, and the process of data exchange, including a description of the data security measures.

http://dti.delaware.gov/pdfs/pp/SecureFileTransport.pdf and
http://dti.delaware.gov/pdfs/pp/DataClassificationPolicy.pdf

b) **Encryption at Rest**: For engagements where the Service Provider stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. The policy document is located at: http://dti.delaware.gov/pdfs/pp/WebApplicationSecurity.pdf. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Service Provider's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, they must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach in accordance with the Cloud and Offsite Hosting Policy, http://dti.delaware.gov/pdfs/pp/CloudandOffsiteHostingPolicy.pdf. Additionally, where encryption of data at rest is not possible, the vendor must describe existing security measures that provide a similar level of protection.

5. **Breach Notification and Recovery**: Delaware Code requires public breach notification when citizens' personally identifiable information is lost or stolen. (Reference: 6 Del. C. § 12B-102. http://delcode.delaware.gov/title6/c012b/index.shtml) Additionally, unauthorized access or disclosure of non-public data is considered to be a breach. The Service Provider will provide notification without unreasonable delay and all communication shall be coordinated with the State of Delaware. When the Service Provider or their sub-contractors are liable for the loss, the Service Provider shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least three (3) years, mailing costs, website, and toll free telephone call center services. The State of Delaware shall not agree to any limitation on liability that relieves a Contractor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Contractor harmless.

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

7. **Termination and Suspension of Service:** In the event of termination of the contract, the Service Provider shall implement an orderly return of State of Delaware data in CSV or XML or another mutually agreeable format. The Service Provider shall guarantee the subsequent secure disposal of State of Delaware data.

a) **Suspension of Services**: During any period of suspension or contract negotiation or disputes, the Service Provider shall not take any action to intentionally erase any State of Delaware data.

b) **Termination of any Services or Agreement in Entirety**: In the event of termination of any services or agreement in entirety, the Service Provider shall not take any action to intentionally erase any State of Delaware data for a period of ninety (90) days after the effective date of the termination. After such 90 day period, the Service Provider shall have no obligation to maintain or provide any State of Delaware data and shall thereafter, unless legally prohibited, dispose of all State of Delaware data in its systems or otherwise in its possession or under its control as specified in section 7d) below. Within this ninety (90) day timeframe, vendor will continue to secure and back up State of Delaware data covered under the contract.

c) **Post-Termination Assistance**: The State of Delaware 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 Service Level Agreement.

d) **Secure Data Disposal**: When requested by the State of Delaware, the provider shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable according to National Institute of Standards and Technology. The policy document is located at:
http://dti.delaware.gov/pdfs/pp/DisposalOfElectronicEquipmentAndStorageMedia.pdf

8. **Background Checks:** The Service Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who has been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for a minimum of one (1) year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.

9. **Data Dictionary:** Prior to go-live,[3] the Service Provider shall provide a data dictionary in accordance with the State of Delaware Data Modeling Standard at
http://dti.delaware.gov/pdfs/pp/DataModelingStandard.pdf

10. **Security Logs and Reports:** The Service Provider shall allow the State of Delaware access to system security logs that affect this engagement, its data and or processes. This includes the ability for the State of Delaware to request a report of the records that a specific user accessed over a specified period of time.

11. **Contract Audit:** The Service Provider shall allow the State of Delaware to audit conformance including contract terms, system security and data centers as appropriate. The State of Delaware may perform this audit or contract with a third party at its discretion at the

---

[3] In this instance, "go live" means that if your organization is awarded the contract, for Delaware data only, upon approval by the State, and before the first data exchange. If your organization wishes to claim this information as proprietary and confidential, follow the directions in Section I.F., *Confidentiality of Documents*.

State's expense. Such reviews shall be conducted with at least thirty (30) days advance written notice and shall not unreasonably interfere with the Service Provider's business.

12. **<u>Sub-Contractor Disclosure</u>:** The Service Provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, who will be involved in any application development and/or operations.[4]

13. **<u>Operational Metrics</u>:** The Service Provider and the State of Delaware shall reach agreement on operational metrics and document said metrics in the Service Level Agreement.[5]

    Examples include but are not limited to:

    a) Advance notice and change control for major upgrades and system changes

    b) System availability/uptime guarantee/agreed-upon maintenance downtime

    c) Recovery Time Objective/Recovery Point Objective

    d) Security Vulnerability Scanning

---

[4] Subcontractors are subject to <u>all</u> the terms and conditions of the RFP. If a subcontractor(s) is involved, note in your response to this question and complete Appendix I, *Subcontractor Information Form*, included herein for <u>each</u> subcontractor.

[5] For this product, the terms would be in the contract's statement of work or performance guarantees.

DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION
CERTIFICATE OF DATA DESTRUCTION
By External Entity/Company

The information described below was destroyed in the normal course of business pursuant to the State of Delaware retention schedule and the following policies and contract(s):

- The Delaware Information Security Policy, Disposal of Electronic Storage Media:
  http://dti.delaware.gov/pdfs/pp/StateOfDelawareInformationSecurityPolicy.pdf

- Data Classification Policy:
  http://dti.delaware.gov/pdfs/pp/DataClassificationPolicy.pdf

- Disposal of Electronic/Storage Media Policy:
  http://dti.delaware.gov/pdfs/pp/DisposalOfElectronicEquipmentAndStorageMedia.pdf

- **Request for Proposal (RFP) for Vision Insurance Benefit, May 26, 2015**:
  On or before August 31, 2016, Company will destroy all data files received for the purpose of implementing the State's vision benefit program. The data is to be used for testing purposes only and will be a file(s) of a sampling of active employees and pensioners. Company will send a certified letter to the DTI Chief Security Officer indicating the date, time and confirmation of the destruction along with this completed form and any documentation produced from the data destruction/data wipe software such as a certificate or certification log. Send via certified mail (or by a delivery service such as UPS or FedEx with a signature receipt required) to: Delaware Department of Technology and Information, Office of the Chief Security Officer, 801 Silver Lake Blvd., Dover, DE 19904 (302-739-9500) with a copy via regular mail to: State of Delaware OMB, Statewide Benefits Office, Attn: Laurene Eheman, 500 W. Loockerman St., Suite 320, Dover, DE 19904.

Company Name and Address:		
Date of Destruction:	Authorized By:	
Description of Information Disposed of/Destroyed: For the purpose of implementation of the State's vision benefit program and for testing purposes only, a file of a sampling of active employees and pensioners. Additional data, if any:		
Inclusive Dates Covered: 2016		
METHOD OF DESTRUCTION: ☐ Burning ☐ Overwriting	☐ Pulping ☐ Pulverizing ☐ Reformatting	☐ Shredding ☐ Other:
Records Destroyed By*:		
If On Site, Witnessed By:		
Department Manager:		

If the records are destroyed by an outside firm, provide the company name and address and confirm that a contract exists.