State of Delaware
Office of Management & Budget
Statewide Benefits Office

STATE EMPLOYEE BENEFITS COMMITTEE

Request for Proposal for the State of Delaware's Supplemental Insurance Program: Group Accident, Cancer, and Critical Illness

November 26, 2014

Addendum #3

OMB14003 – SuppIns

500 W. Loockerman Street, Suite 320 • Dover, DE 19904
Phone (800) 489-8933 Fax (302) 739-8339 www.ben.omb.delaware.gov

The following terms are additional minimum requirements to those in Section V, Technical Standards and Security Requirements.

Subcontractors: Subcontractors are subject to all the terms and conditions of the RFP. If your organization identified a subcontractor for technology services, the subcontractor must respond to the following requirements.

1. SSL vs. TLS

On October 14, 2014, Microsoft issued security advisory 3009008 (https://technet.microsoft.com/en-us/library/security/3009008.aspx) to address serious vulnerabilities with SSL 3.0. As a result, the Office of Management and Budget (OMB) and many other State agencies have programmatically disabled SSL for desktop browsers. Secure sessions should now use TLS 1.0, TLS 1.1 or TLS 1.2. Will this affect the use of your product? Please provide a response with a detailed explanation.

Response:

2. Terms and Conditions:

Any vendor that receives the State's data via the internet and is an external host of the State's data is deemed to be a Software as a Service (SaaS) cloud provider and must comply with the related State security protocols, standards, and terms. Because the selected vendor for the Supplemental Insurance Program will be storing the State's data, the State considers the vendor an external host and therefore a cloud provider.

The terms are mandatory for every engagement. Exceptions will be considered non-compliant and non-responsive. However, the State understands that data ownership resides with the vendor on a fully-insured product. If you assert that a term does not apply due to a data ownership term or to the technology services required in this RFP, or you want to provide information about your organization's alternative solution to provide the required service, please complete the attached *Technology Exception Tracking Chart* with a detailed explanation. You may not respond that a term is not applicable because you are not a cloud provider.

A. **Data Protection**: Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Service Provider (vendor) 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 condition: 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.

   Response:

B. **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.

   Response:

C. **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.

1. 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.

2. 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 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. Within this 90 day timeframe, vendor will continue to secure and back up State of Delaware data covered under the contract.

3. 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.

Response:

D. **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 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.

Response:

E. **Operational Metrics**: The Service Provider and the State of Delaware shall reach agreement on operational metrics and document said metrics in the Service Level Agreement (contract). Examples include but are not limited to:

1. Advance notice and change control for major upgrades and system changes

2. System availability/uptime guarantee/agreed-upon maintenance downtime

3. Recovery Time Objective/Recovery Point Objective

4. Security Vulnerability Scanning

Response:

3. Data Confidentiality Agreement

Question #58, Page 29, is deleted and replaced with the following Minimum Requirement.

The file feeds that are not specific to the University of Delaware originate with the State's Payroll Human Resources Statewide Technology ("PHRST") system. The attached *Data Confidentiality Agreement* must be executed by the awarded vendor and will be included as an attachment to the contract. Please indicate your agreement or provide a red-lined document with suggested changes for the State's consideration. The State will not agree to revisions that circumvent the purpose of the agreement.

Response:

4. Single Sign On (SSO)

Authentication: Configuration of Single Sign-on (SSO) integrated with Oracle Identity Access Management (IAM), 11g R2 using SAML 2.0 protocol.

Response:

(continued on next page)

Appendix A

TECHNOLOGY EXCEPTION TRACKING CHART

Responses must include all exceptions to the specifications, terms or conditions contained only in the Addendum #3. If the vendor is submitting the response without exceptions, please state so below.

☐ By checking this box, the vendor acknowledges that they take no exceptions to the specifications, terms or conditions found in Addendum #3.

Page and ? #s	(Copied) Term	Detailed Exception	Proposed Alternative, if different

OMB14003-SuppIns
Supplemental Insurance Program – Group Accident, Cancer, and Critical Illness

DATA CONFIDENTIALITY AGREEMENT

This Data Confidentiality Agreement ("Agreement") is undertaken pursuant to the parties' performance of a certain contract ("Contract") effective July 1, 2015, 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 or other covered persons and _____ _____ ("Contractor"), with offices at _____ _____.

WHEREAS, State desires to obtain certain software and services of Contractor;

WHEREAS, Contractor desires to provide such software and services to State on the terms set forth below and within the Contract;

WHEREAS, 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, State and Contractor agree as follows:

This Agreement constitutes an agreement undertaken by and between the State by and through Payroll Human Resources Statewide Technology ("PHRST") and Contractor.

1. PURPOSE
   The Contract provides for a PHRST data extract to Contractor at regular intervals. The data contained in the PHRST data extract files ("PHRST Data") is to be used exclusively to populate the Contractor's system and is not to be used for any other purpose.

2. DEFINITIONS
   a. State of Delaware Secret: Information that, if divulged, could compromise or endanger the people or assets of the State and data that is specifically protected by law.

   b. Personally Identifiable Information (PII): Information which can be used to identify or contact a person uniquely and reliably, or can be used with other sources to uniquely identify an individual. Examples include, but are not limited to, full name, full social security number, employee identification number ("EmplID"), full date of birth, street address, telephone number, and email address.

3. CLASSIFICATION OF DATA
   The PHRST Data being provided under the Agreement is classified "State of Delaware Secret" in accordance with the Department of Technology and Information ("DTI") Data Classification Policy. The combination of the data elements in the PHRST Data file meet the definition of Personally Identifiable Information (PII) as defined in the DTI Data Classification Policy.

4. METHOD OF DATA ACCESS AND TRANSFER
   The PHRST Data will be generated in a pre-defined comma delimited file format automated Cybermation schedule. As part of this automated process the file will be placed on the Contractor's production SFTP server (ftp.stateofdelaware.csod.com) in the /datafeed/ folder using previously exchanged SSH key provided by STATE. The file will be encrypted using the also previously exchanged PGP key provided by Contractor. Contractor is responsible to obtain the file from their server, decrypt, and import into the Contractor's system.

5. FREQUENCY OF DATA EXCHANGE
   PHRST Data will be exchanged at a regular interval set forth in the Contract.

6. RETENTION/LIFECYCLE OF DATA
   PHRST Data transmitted pursuant to this Agreement shall be retained so long as necessary to achieve its intended purpose. Contractor agrees to secure such data until such time as it may be destroyed or deleted within the terms set forth in the Contract.

7. NON-DISCLOSURE OF DATA
   a. Contractor's employees or sub-contractors shall not disclose, in whole or in part, the data described in this Agreement to any individual or organization not specifically authorized by this Agreement or the Contract.

   b. Contractor is required to comply with all applicable confidentiality-related Federal, State and Local laws.

   c. Notwithstanding any other provision of this agreement, PHRST shall be considered the custodian of the data it provides to Contractor for the purposes of the State Freedom of Information Act ("FOIA"), 29 *Del. C.* Ch. 100. All requests pursuant to FOIA for data subject to this Agreement in the possession of Contractor must be referred to PHRST. To the extent that Contractor modifies the form or content of data disclosed by PHRST, Contractor shall be considered the custodian of such information for the purposes of FOIA.

8. DATA BREACH
   Any breach in the security or confidentiality of the data being shared shall be reported immediately to PHRST and to the DTI Security Office within the timeframe and manner as set forth in the Contract.

No clause of this Agreement shall be considered a waiver of any portion of the Contract as previously executed between Contractor and the State.

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 duly executed as of the date and year first above written.

STATE OF DELAWARE **OFFICE OF MANAGEMENT AND BUDGET**	**CONTRACTOR**
_____ Signature	_____ Signature
Brenda L. Lakeman Director of HR Management and Benefits Administration	Printed Name: Title:
_____ Date	_____ Date