STATE OF VERMONT CONTRACT SUMMARY AND CERTIFICATION - - - - - - - - - - - Form AA-14 (1/8/2019)

Note: All sections must be completed. Incomplete forms will be returned to the originating department.

I. CONTRACT INFORMATION:

Agency/Department: Green Mountain Care Board/ **Contract #:** 38739 **Amendment #:**

Vendor Name: Onpoint Health Data VISION Vendor No**:** 286356

Vendor Address: 75 Washington Ave., Ste 1E, Portland, ME 04101

Starting Date: 8/15/19 **Ending Date:** 8/14/2024 **Amendment Date:**

Summary of agreement or amendment: Vermont Healthcare Claims Uniform Reporting and Evaluation System (VHCURES), Vermont's All-Payer Claims Database (APCD).

II. FINANCIAL & ACCOUNTING INFORMATION

Maximum Payable: $4,619,800.00 Prior Maximum: $ Prior Contract # (If Renewal): 20229

Current Amendment: $ Cumulative amendments: $ % Cumulative Change:

Business Unit(s): 3330; ; - [notes:] **VISION Account(s):** ;

Estimated Funding Split:	40.00 % GF	60.00 % SF	% EF	% Other (name)
	% TF	% GC	% FF	

III. PROCUREMENT & PERFORMANCE INFORMATION

A. Identify applicable procurement process utilized.

☒ Standard Bid/RFP ☐ Simplified ☐ Sole Source (See B.) ☐ Qualification Based Selection ☐ Statutory

B. If Sole Source Contract, contract form includes self-certification language? ☐ Yes ☒ N/A

C. Contract includes **performance measures/guarantees** to ensure the quality and/or results of the service? ☒ Yes ☐ No

IV. TYPE OF AGREEMENT (select all that apply)

☐ Personal Service
☒ Non-Personal Service
☐ Commodity

☐ Construction ☐ Arch/Eng. ☐ Marketing ☐ Info. Tech. ☒ Prof. Service

☐ Retiree/Former SOV EE ☐ Financial Trans ☐ Zero-Dollar ☐ Privatization ☐ Other

V. SUITABILITY FOR CONTRACT FOR SERVICE

☒ Yes ☐ No ☐ n/a Does this contract meet the determination of an Independent Contractor? If "NO", the contractor must be set up and paid on payroll through the VTHR system.

VI. CONTRACTING PLAN APPLICABLE

Is any element of this contract subject to a pre-approved Agency/Dept. Contracting Waiver Plan? ☐ Yes ☒ No

VII. CONFLICT OF INTEREST

By signing below, I (Agency/Dept. Head) certify that no person able to control or influence award of this contract had a pecuniary interest in its award or performance, either personally or through a member of his or her household, family, or business.

☐ Yes ☒ No Is there an "appearance" of a conflict of interest so that a reasonable person may conclude that this party was selected for improper reasons: (If yes, explain)

VIII. PRIOR APPROVALS REQUIRED OR REQUESTED

☒ Yes ☐ No Agreement must be Certified by the Attorney General under 3 V.S.A. § 342 (sign line #4 below)
☒ Yes ☐ No Attorney General review As To Form is required ($25,000 and above) or otherwise requested:_____ (AAG initial)
☒ Yes ☐ No Agreement must be approved by the Secretary of ADS/CIO
☐ Yes ☒ No Agreement must be approved by the CMO: for Marketing services over $25,000
☐ Yes ☒ No Agreement must be approved by Comm. Human Resources: for Privatization, Retirees, Former Employees, & if a Contract fails the IRS test.
☒ Yes ☐ No Agreement must be approved by the Secretary of Administration

IX. AGENCY/DEPARTMENT HEAD CERTIFICATION; APPROVAL

I have made reasonable inquiry as to the accuracy of the above information (sign in order):

1-Date	1-Agency/Department Head	2-Date	2-Agency Secretary (if required)
	E-SIGNED by Susan Barrett on 2019-07-29 16:40:49 GMT		

3a-Date	3a-CIO	3b-Date	3b-CMO	3c-Date	3c-Commissioner DHR
	E-SIGNED by John Quinn on 2019-08-07 01:47:16 GMT				

4-Date	4-Attorney General	5-Date	5-Secretary of Administration
	E-SIGNED by Jesse Moorman on 2019-07-30 20:03:55 GMT		E-SIGNED by Brad Ferland on 2019-08-12 18:39:49 GMT

E-SIGNED by Kelly Murphy on 2019-08-07 14:48:50 GMT

STANDARD CONTRACT FOR TECHNOLOGY SERVICES

1. *Parties*. This is a contract for services between the State of Vermont, Green Mountain Care Board (hereinafter called "State" or "GMCB"), and Onpoint Health Data, with a principal place of business in 75 Washington Avenue, Ste. 1E, Portland, Maine 04101, (hereinafter called "Onpoint" or "Contractor"). Contractor's form of business organization is non-profit corporation under Section 501 (c)(3) of the Internal Revenue Code. It is Contractor's responsibility to contact the Vermont Department of Taxes to determine if, by law, Contractor is required to have a Vermont Department of Taxes Business Account Number.

2. *Subject Matter*. The subject matter of this contract is services generally on the subject of development and design services, project and operations management, support and maintenance, consulting, training, engineering and application development, monitoring, support, backup and recovery, change management, technology updates and upgrades and other professional services as described herein (individually and collectively referred to herein as the "Services"), as necessary for the State's productive use of the Solution, the Vermont Healthcare Claims Uniform Reporting and Evaluation System (VHCURES), Vermont's All-Payer Claims Database (APCD). Detailed services to be provided by Contractor are described in Attachment A.

3. ***Maximum Amount***. In consideration of the services to be performed by Contractor, the State agrees to pay Contractor, in accordance with the payment provisions specified in Attachment B, a sum not to exceed $4,619,800.00.

4. ***Contract Term.*** The period of Contractor's performance shall begin on August 15, 2019 and end on August 14, 2024. This contract may be renewed for two additional 12-month periods, as agreed by both parties and reduced to a written amendment.

5. ***Prior Approvals*.** This Contract shall not be binding unless and until all requisite prior approvals have been obtained in accordance with current State law, bulletins, and interpretations.

6. ***Amendment.*** No changes, modifications, or amendments in the terms and conditions of this contract shall be effective unless reduced to writing, numbered and signed by the duly authorized representative of the State and Contractor.

7. ***Termination for Convenience*.** This contract may be terminated by the State at any time by giving written notice at least thirty (30) days in advance. In such event, Contractor shall be paid under the terms of this contract for all services provided to and accepted by the State prior to the effective date of termination.

8. ***Attachments***. This contract consists of 68 pages including the following attachments which are incorporated herein:

Attachment A – Statement of Work
- Exhibit 1 – State Technical and Functional Requirements
- Exhibit 2 – Preliminary Implementation Master Schedule
- Exhibit 3 – Operational Tasks/Payment Schedules
- Exhibit 4- Third Party Software Licensed the State of Vermont

Attachment B – Payment Provisions
Attachment C – Standard State Provisions for Contracts and Grants a preprinted form (revision date 12/15/2017)
Attachment D – Other Terms and Conditions for Information Technology Contracts
Attachment E – Maintenance and Support/Service Level Terms
Attachment F – Delivery Expectation Document (DED) and Delivery Acceptance Form (DAF)

9. ***Order of Precedence***. Any ambiguity, conflict or inconsistency between the documents comprising this contract shall be resolved according to the following order of precedence:

1) Standard Contract
2) Attachment D Other Terms and Conditions for Information Technology Contracts
3) Attachment C (Standard State Provisions for Contracts and Grants)
4) Attachment A with Exhibits
5) Attachment B
6) Attachment E
7) Attachment F

WE THE UNDERSIGNED PARTIES AGREE TO BE BOUND BY THIS CONTRACT

By the State of Vermont:

Date: E-SIGNED by Kevin Mullin on 2019-08-13 15:04:25 GMT

Signature: _____

Name: _____

Title: _____

Onpoint Health Data:

Date: E-SIGNED by Jim Harrison on 2019-08-13 14:53:03 GMT

Signature: _____

Name: _____

Title: _____

ATTACHMENT A
SPECIFICATIONS OF WORK TO BE PERFORMED

1. PURPOSE

This Contract sets forth the terms and conditions under which Contractor agrees to provide to the State a Contractor-supported Vermont All-Payer Claims Database (VHCURES) (the "Solution"). The Solution shall provide development and design services, project and operations management, support and maintenance, consulting, training, engineering and application development , monitoring, support, backup and recovery, change management, technology updates and upgrades and other professional services as described herein (individually and collectively referred to herein as the "Services"), as necessary for the State's productive use of the Solution, as further set forth in this Contract. This Contract specifies the obligations of each party with additional provisions detailed in the accompanying Attachments and Exhibits.

2. EXISTING SYSTEMS

The Vermont Legislature first called for the formation of an all-payer claims database in the 1990s, but it was not until 2009 with the enactment of 18 V.SA. 9410 that VHCURES was established. Today, VHCURES is regulated by the State in accordance with Regulation H-2008-01. The Green Mountain Care Board (GMCB) has been responsible for maintaining VHCURES since 2013. The GMCB, created by the Vermont Legislature in 2011, works to ensure that the Vermont health care system provides quality, affordable health care to all Vermonters while reducing waste and controlling costs. To achieve these goals, the Green Mountain Care Board's priorities are focused on:

- Overseeing a health care payment and delivery system designed to improve the quality of care while reducing costs
- Monitoring and exerting downward pressure on overall health care spending
- Developing programs and creating partnerships to assess and enhance quality and safety in the health care system
- Enhancing system transparency and consumer involvement.

The GMCB works closely with other state agencies, the Legislature, the Vermont business community, health care professionals and providers, and the citizens of Vermont to carry out its unique mission. In addition to VHCURES, the GMCB also oversees the State's hospital budgets and health insurance rates among other responsibilities. In 2014, the approved the implementation of a Data Governance and Stewardship Program. Central to the program is the Data Governance Council which oversees data stewardship in areas of data quality to promote the highest possible quality of GMCB's data resources, risk pertaining to data privacy and security, financial sustainability of the GMCBs data stewardship program, and data release to support clear processes for the evaluation of data requests and the release of data to State and non-State research entities.

Statutorily, the GMCB is required to maintain the VHCURES database for a variety of purposes, including: (1) determining the capacity and distribution of existing state resources; (2) identifying health care needs and informing health care policy; (3) evaluating the effectiveness of intervention programs for improving patient outcomes; (4) comparing costs between various treatment settings and approaches; (5) providing information to consumers and purchasers of health care; and (6) improving the quality and affordability of patient health care and health care coverage.

3. OBJECTIVE

This Contract identifies the tasks required by each party to implement and support the Solution through the following major activities: development of project management planning documentation; requirements collection and validation; Solution design; data migration, configuration, integration and testing; deployment and training; and operations, support, and maintenance services, all as detailed herein.

The project will be executed in phases as described herein.

The successful outcome of the project is defined by the following:

- Completed in accordance with this Contract and applicable project management planning documentation;
- Resolved all material functional and operational deficiencies prior to deployment in the production environment;
- Completed within budget;
- Configured to meet all specified requirements and needs of the State;
- The Solution meets and adheres to all requirements and timeframes set forth in service level terms set forth herein;
- The Solution is fully documented, including but not limited to requirements specifications, architecture, design, configuration, operational environment and user manuals; and
- Trained State staff and stakeholders.

3.1 PERIOD OF INSTALLATION AND IMPLEMENTATION AND TRAINING

3.2 DEFINITIONS

The period of installation and implementation and training shall not exceed 13 months from the start date of this Contract. Support and maintenance shall begin upon Solution deployment and shall continue through the Contract Term as the same may be extended by the parties.

Capitalized terms used in this Contract not specifically defined in the text shall have the following meanings:

(a) **"Certificate of Acceptance"** means written certification, delivered to Contractor and signed by an authorized representative of the State, stating that any Defects in a particular Phase or the Solution discovered after implementation and testing have been corrected as required under this Contract, and that the Phase complies in all material respects with all of the applicable Requirements.

(b) **"Certificate of Completion"** means written certification, delivered to the State and signed by an authorized representative of Contractor, stating that any Defects in a particular Phase or the Solution discovered after implementation, testing and Acceptance have been corrected as required under this Contract, and that the Phase or Solution complies in all material respects with all of the applicable Solution Requirements. The State must provide written acceptance to Contractor of any and all Certificates of Completion for them to become effective.

(c) "**Contractor Personnel**" means and refers to Contractor's employees and employees of Contractor's permitted subcontractors or permitted agents assigned by Contractor to perform Services under this Contract.

(d) **"Defect"** means any failure by the Solution or any Phase or component thereof to conform in any

material respect with applicable Requirements.

(e) **"Defect Correction"** means either a modification or addition that, when made or added to the Solution, establishes material conformity of the Solution to the applicable Requirements, or a procedure or routine that, when observed in the regular operation of the Solution, eliminates the practical adverse effect on the State of such nonconformity.

(f) "**Documentation**" means any and all descriptions and specifications of the Requirements included herein or created or developed hereunder, operational, functional and supervisory reference guides, manuals and instructive materials, in whatever form and regardless of the media on which it may be contained, stored or transmitted, which is developed, prepared, used or otherwise available from Contractor and/or Contractor's suppliers, in connection with and applicable to the provision, use, operation and support of the Services hereunder. Documentation shall be sufficient to enable State personnel to understand, operate, use, access, support, maintain, update and modify Services, notwithstanding that Contractor is or may be responsible for any or all of the foregoing obligations. Documentation shall also include all standards applicable to the Services, including those applicable to: (i) Contractor for its own comparable items or services; (ii) the State for its own comparable items or services; and (iii) such standards and guidelines as the parties mutually agree apply to the Services involved.

(g) "**Final Acceptance**" means the issuance of Certificate of Acceptance executed by the State which specifies the mutually agreed upon Go Live Date for the Solution.

(h) "**Facilities**" means the physical premises, locations and operations owned or leased by the State (a "State Facility") or the Contractor (a "Contractor Facility"), and from or through which the Contractor and/or its permitted contractors will provide any Services.

(i) **"Go Live Date."** The date that the all or any part of the entire Solution is first available for use by the State in an operational, non-test environment, utilizing actual production data.

(j) "**Phases."** A particular portion of the Solution, as set forth in the Implementation Master Schedule or as may be modified in accordance with this Contract. Unless modified by written agreement of the parties, the five project Phases are Solution Definition and Design, Requirements Gathering, Customization, Deployment, Training and Maintenance and Support.

(k) "**Requirements**" means the State's baseline Functional and Technical Requirements attached as Exhibit 1 to Attachment A of this Contract.

(l) "**Service Level**" means the specific level of performance Contractor is required to comply with and adhere to in providing the Services in conformity with the Requirements, consistent with the criteria and parameters specified in this Contract. Service Level Terms are set forth in Attachment E to this Contract.

4. PROJECT MANAGEMENT

The scope of work as detailed below describes the services, deliverables and key assumptions. Contractor will develop an overall project schedule that details the tasks, timelines, and deliverables for the fully integrated solution.

4.1 CONTRACTOR PROJECT MANAGEMENT AND SUPPORT

4.1.1 CONTRACTOR'S PROJECT MANAGER

Contractor will designate an individual to serve as the "**Contractor Project Manager**" who will: (i) be a senior employee within Contractor's organization, with the information, authority and resources available to properly discharge the responsibilities required hereunder; (ii) serve as primary point of contact and the single-point of accountability and responsibility for all Contract-related questions and issues and the provision of Services by Contractor; (iii) have day-to-day responsibility for, and authority to manage, State customer satisfaction; (iv) devote the required time and dedicated efforts to managing and coordinating the Services; and (v) be located at State Facilities or such other appropriate location as Contractor and the State may mutually agree.

Contractor's Project Manager shall be responsible for all tasks necessary to manage, oversee, and ensure success of the project. These tasks shall include but are not limited to participating in the following; development and updating of project plans, assigning contract staff, scheduling meetings, developing and publishing status reports, addressing project issues, risks, and change orders, and preparing presentations for the State.

Contractor's Project Manager shall be responsible for the successful delivery of all Contractor tasks and subtasks defined in within this contract, deliverables, and documentation through the lifecycle of the project. Progress will be monitored and plans adjusted, as necessary, in project status meetings.

The following table identifies the documentation to be established, maintained, and managed to;

Deliverable	Description	Update Frequency	Lead Assigned
Project Management Plan	The Project Management Plan will dictate specifics on how the Contractor Project Manager will administer the project and will include the following documentation: 1. Change Management Plan (will dictate how changes will be handled including any Service level terms on over/under estimates) 2. Communication Management Plan (will dictate what will be communicated, to who, and how often) 3. Requirements Management Plan (will dictate the approach that the requirements will be gathered, approved, and maintained)	Once unless there are changes	State PM

Deliverable	Description	Update Frequency	Lead Assigned
	4. Risk and Issues Management Plan (will dictate how risks and issues will be managed over the course of the project) 5. Scope Management Plan (will dictate how the scope will be maintained to prevent "scope creep") 6. Test Plan (will dictate the testing approach, participants, sequence of testing and testing preparations. (Test plans will be developed by the SOV.)		
Transition to Operations Plan	Transition to Operations Plan	Once unless there are changes	State PM with input from Contract PM
Deliverable Expectation Document (DED)	Criteria that establishes the acceptance and rejection criteria for each document on this list.	Once per phase/milestone	Contract PM
Deliverable Acceptance Form (DAF)	Obtain sign-off at the completion of each project deliverable as defined by the formal acceptance criteria.	Once per phase/milestone	Contract PM
Change Requests	Formal document which outlines any changes to the Contract scope, schedule, budget, and resources.	As needed	PM of requesting Party
Project Log	Project log is a spreadsheet that has a tab for each of the following items: • Risks: Tracking of potential impacts to the project. • Issues: Tracking of risks which have escalated into an issue, or issue identified, through resolution. • Changes: Tracking the change request documents submitted through evolution. • Action Items: Tracking all tasks identified as a breakdown of the IMS, through meetings, or conversations. • Decisions: Tracks all decisions made over the course of the project. Decisions must identify when the decision was made and who authorized its approval. • Budget: Outlines Contract costs by deliverable paid-to-date information, as well as other State obligations to maintain. (SOV PM Only)	Minimum of Weekly	State PM with input from Contract PM

Deliverable	Description	Update Frequency	Lead Assigned
Requirements Traceability Matrix (RTM)	Finalized list of the project requirements to be met through the successful completion of this project. The finalized requirements will be provided to the Contract PM for mapping to deliverables, gap identification, and RTM document management.	Aligned with DED & DAF submission/ approval	State PM to establish, Contract PM to manage
Test Cases & Results	The specific test cases to be tested and the testing results. Test Cases tie back to the project requirements (to ensure each one has been met).	Create once then update with Results	State PM
Implementation Master Schedule	The IMS outlines how the project will go-live the exact events that need to occur assigned to the resources that need to do them and the timeframe for when they need to get done. (See Section 4.3 for more detail.)	Once per implementation	Contract PM
Project Schedule (MPP)	The evolved IMS outlining the scheduled events as known and updated through the project lifecycle.	Weekly	State PM with input from Contract PM
Project Status Reports	Provides an update on the project status, accomplishments, noteworthy decisions made, upcoming tasks, risks and significant issues. The Status Report and the project color being report shall be developed in consultation with the State project manager, as set forth in greater detail in Section 4.2.3. The state PM will be the creator and owner, the contractor PM will work with the State PM to create it, aka provide inputs to it.	Weekly	State PM
Meeting Agenda/ Minutes	All scheduled meetings will have an agenda and minutes. The minutes shall contain risks, issues, action items, and decisions.	Agenda: At least 8 business hours prior to occurrence. Minutes: within 24 business hours after occurrence	State PM who may delegate to Contract PM as needed
Lessons Learned	A compilation of the lessons learned having 20/20 hindsight. This shall include project team members, stakeholders, and other parties as they were involved and is deemed necessary to obtain a full 360-degree view of the project in retrospect.	Once	State PM with input from Contract PM

Deliverable	Description	Update Frequency	Lead Assigned
Closeout Report	This report will include all the lessons learned, project metrics, and a summary of the project's implementation and outcome in operation.	Once	State PM with input from Contract PM

Documents produced shall use State existing templates, unless otherwise approved by the State project manager.

Contractor's Project Manager shall assist the State's Project Manager (upon request) in creating and updating the documentation listed and/or materials for periodic presentations to State project sponsors and key stakeholders. Contractor's Project Manager may be required to present information to, and answer questions from, State stakeholders at these presentations.

4.1.2 PROJECT MANAGEMENT AND SUPPORT

The Contractor will apply project management processes based on PMI (Project Management Institute's PMBOK) principles to ensure on-time and within-budget delivery of the Solution, while meeting all the requirements in this Contract. The State will approve all project management methods and tools used during the project. These project management methods and tools are considered project deliverables.

4.1.3 KEY PROJECT STAFF

Contractor will perform and support the Services consistent with this Contract and the Solution Requirements. Contractor Personnel will be properly educated, trained and qualified for the Services they are to perform, and Contractor will put appropriate training in place to meet initial and ongoing training requirements of Contractor Personnel assigned to perform Services.

(a) Contractor shall be responsible, at its own cost and expense, for any and all recruitment, hiring, Contractor-specific training, education and orientation for all Contractor Personnel assigned or to be assigned to perform Services or support the Requirements.
(b) All Contractor Personnel, in addition to any Contractor security policies and procedures, shall be required to comply with the security requirements in this Contract.
(c) Contractor shall conduct its hiring process in compliance with all applicable Federal and State laws to include, but not be limited to, anti-discrimination laws.

(i) **Eligibility for Employment:** Contractor shall verify that all prospective employees are eligible for employment in the United States.
(ii) **Criminal Records:** Contractor or an agent of Contractor shall perform criminal background checks on all prospective employees utilizing a national criminal database acceptable to the State. Before any Contractor Personnel begin work on the Services x) such background check shall have returned a "no record" result or, y) to the extent that the result revealed that a felony record or records exist for a given individual, the associated conviction(s) shall be unrelated to the work to be performed as specified under the Equal Employment Opportunities Commission's EEOC Enforcement Guidance regarding the employment of convicted felons issued April 25, 2012. Contractor shall provide the State with notice of proposed Contractor Personnel with felony or misdemeanor convictions that involve a crime against a person; a crime involving the use or misuse of computer network; a crime involving weapons, explosives or arson; a crime involving trade secret/proprietary information; a crime involving theft, dishonesty, embezzlement, breach of fiduciary

duty, identity theft, or other financial-related crimes; a felony conviction for drug possession; or a crime involving the distribution or trafficking of illegal drugs and/or controlled substances.

(d) All Contractor Personnel providing or assigned to provide Services or otherwise in a position to obtain or have access to State Information, shall execute a non-disclosure agreement in a form acceptable to the State.

(e) The timing for transfer, reassignment or replacement of Contractor Personnel will be coordinated with requirements for timing and other elements of the Services so as to maintain continuity in the performance of the Services and avoid interruption or disruption to the Services or any failures to maintain Service Levels.

Contractor shall assign the following Contractor staff ("Key Project Staff"), to meet the Requirements of this Contract:

Project Role	Name	Title
Dedicated Project Manager	Carolyne Conrad	Client Account Manager
Lead Client Support	Janice Bourgault, CPC	Senior Director of Client Services
Operations Management & Quality Assurance Lead	Joanna Duncan, PhD, CPC	Director of Data Analytics & Operations
Technical Infrastructure Lead	Corey Ramsey	Manager of IT
Data Security Officer	Ramzi Saba	Chief Information Officer
Analytic Solution Lead	Karl Finison, MA	Director of Analytic Development
System Development Lead	Jeff Cain	Lead Systems Developer
Data Analyst Lead	Sam Chick	Senior Health Data Analyst
Dedicated Operations Analyst	Dawn Hamlin	Operations Analyst
Dedicated Data Analyst	Adam Bakopolus	Health Data Analyst

Contractor will cause the Contractor Personnel filling the Key Project Staff positions to devote the required time and dedicated effort to the provision of the Services and the achievement of Service Levels required for the Services, unless a lesser allocation during certain Project Phases may be agreed in writing.

4.1.4 KEY PROJECT STAFF CHANGES

Contractor shall not change the project assignment of Carolyne Conrad, Janice Bourgault, Joanna Duncan, Corey Ramsey, Ramzi Saba, Karl Finison, Jeff Cain, Sam Chick, Dawn Hamlin, and Adam Bakopolus for the period of project implementation. Contractor shall not change other members of Key Project Staff without providing the State written justification, a comprehensive transition plan and obtaining prior written approval of the State. State approvals for replacement of Key Project Staff will not be unreasonably withheld.

The replacement of Key Project Staff shall have comparable or greater skills and applied experience than being replaced and be subject to reference and background checks described above. If Contractor removes Key Project Staff for any reason without the State's approval, Contractor agrees to replace the new Key Project Staff member if performance is unacceptable to State and provide the first thirty (30) days of a replacement resource with equivalent skill at no charge.

Notwithstanding the foregoing, the State acknowledges that Key Project Staff may become unavailable due to termination of employment for any reason, through disability or death, illness, or through leave of absence such as FMLA or National Guard duty for example. In such circumstances, Contractor shall promptly notify the State in writing of the impending or actual departure of any Key Personnel and of the qualifications and identity of proposed replacement Key Project Staff. The State has the right to reasonably disapprove of any replacement Key Project Staff.

4.1.5 CONTROL OF CONTRACTOR PERSONNEL.

Contractor shall be fully responsible for the management, compensation, and performance of all Contractor Personnel, and the filing of any and all returns and reports and the withholding and/or payment of all applicable federal, State, and local wage tax, or employment-related taxes, including, but not limited to, income taxes, gross receipt taxes, taxes measured by income, social security taxes, and unemployment taxes for Contractor and Contractor's employees. Notwithstanding the foregoing, Contractor's employees shall adhere to the State's policies and procedures, of which Contractor is made aware, while on State Premises, and shall behave and perform in a professional manner. The State, may, in its reasonable discretion, require Contractor to replace any Contractor Personnel, including but not limited to Key Project Staff, working hereunder who does not adhere to, behave, and perform consistent with the State's policies and procedures, or otherwise engages in unprofessional or unethical conduct, or abuses any illegal substance or alcohol, or engages in illegal activities or consistently underperforms. The State shall provide written notice to Contractor of the requirement of replacement, or with whom there are irresolvable personality conflicts. Contractor shall use reasonable efforts to promptly and expeditiously replace Key Project Staff and replace all other personnel within fifteen (15) business days of receipt of the written notice unless otherwise mutually agreed. The State's right to request replacement of Contractor Personnel hereunder relates solely to the removal of individuals from work on this Contract with the State and does not create an employment relationship. Nothing in this Contract authorizes the State to direct the Contractor's termination of the employment of any individual

4.1.6 CONTRACTOR THIRD PARTY CONTRACT

The State acknowledges and understands that Contractor will enter into a third party contracts with the following Contractor subcontractor: Tableau for the performance of Services hereunder. Contractor shall deliver a copy of all such third party contracts to the State for review upon request. The State hereby consents to the use by Contractor of these subcontractors, provided however that any such consent is not deemed acceptance of the terms of any subcontracts by the State.

4.2 PROJECT PLANNING

The State and Contractor Project Managers will arrange for kick-off dates and procedures for managing the project – such as reporting status and resolving issues. This will provide an opportunity to introduce all key members of the project teams and walk through the project management plan and key milestones.

4.2.1 MEETING PROTOCOLS

For regular weekly project status meetings, the State project manager shall provide a meeting agenda and any handouts at least one business day in advance of the scheduled meeting. The Contract project manager may be called upon to perform these duties at the request of the State project manager at any point during the project.

4.2.2 PROJECT DOCUMENT STORAGE

The State will establish a SharePoint site, that is accessible to the Contractor and the State. This will provide a common area for project documents, artifacts, and deliverables to be retained. Access to all SharePoint sites (or other medium of collaboration) and all project material contained therein shall be delivered to the State upon request or completion of the project.

4.2.3 STATUS REPORTS

The status report information shall include, at a minimum: all planned tasks accomplished for the reporting period; planned tasks that are incomplete, or behind schedule in the previous week (with reasons given for those behind schedule); all tasks planned for the upcoming two weeks; an updated status of tasks (entered into the Master Project Work Plan (MPP) and attached to the status report – e.g., percent completed, resources assigned to tasks, etc.); and the status of any corrective actions undertaken. The report will also contain items such as the current status of the project's technical progress and contractual obligations; achievements to date; risk management activities; unresolved issues; requirements to resolve unresolved issues; action items; and identified changes with their status (e.g., pending submission, in review, etc.).

The State Project Manager and Contractor's Project Manager will come to agreement on the exact format of the project documentation and collaboration reports, at or before the project kick-off meeting.

Each report shall include a project dashboard at the top outlining the overall status of the project in terms of the standard triple constraint: cost, time, scope (using a legend or icon of green, yellow, and red based upon the following definitions):

- Green – on track to deliver committed scope by committed deadline with committed resources/funding.
- Yellow – not on track to deliver committed scope by committed deadline with committed resources/funding, but have a plan to get back to green.
- Red – not on track and currently do not have a plan to get back to green. Need project management intervention or assistance.

In the event of yellow or red overall project status, there should be a specific task(s) and/or issue(s) identified as yellow or red which are the root cause of the overall project status being yellow or red. These items shall be presented in sufficient detail to determine the root-cause. The Status Report shall provide a link to the Risks and Issues Log for more detail.

4.3 IMPLEMENTATION MASTER SCHEDULE

The Contractor has compiled a preliminary "baseline" implementation master schedule ("IMS") using the best available knowledge at the time of Contract signing which is attached to this Attachment A as Exhibit 2. The project managers shall work together to implement any IMS changes in accordance with the terms of this Contract; provided, however, in no event shall revisions to the IMS be deemed to amend this Contract. Changes to project scope, term or maximum amount shall require a Contract amendment.

The IMS is an ongoing tool for anticipating and tracking changes to expectations for all project tasks, deliverables and milestones. The complete IMS is an integrated plan – that is, it includes actions and deliverables from all project areas – both Contractor and State. The complete IMS, which includes the detailed tasks and milestones, shall reside in Microsoft Project (.mpp) format (Version 2013 or higher) and will be shared in the ongoing communication meetings to discuss changes. State shall sign off on all

deliverables from each phase of the IMS before subsequent phase work is initiated through the use of the Deliverable Expectation Document and Deliverable Acceptance Form. Once sign off is complete, Contractor and State will assess readiness to proceed with next phase.

5. SCOPE OF SERVICES

5.1 DESCRIPTION OF SERVICES

Contractor agrees to provide and shall perform the Services described herein in accordance with and subject to the terms and conditions set forth in this Contract.

5.2 PROJECT MAJOR PHASES, WARRANTY AND OPTIONS

The Contractor shall, at a minimum, provide State access to a Solution that meets the tools and functionality requirements of the State set forth in Exhibit 1 and Exhibit 3 to this Attachment A. Contractor shall use system development and configuration control methodologies and the desirable sequence of project major phases as described herein. Estimated dates in the following table shall be finalized in the IMS as described in Section 4.3, "Implementation Project Schedule."

5.3 STATE-CAUSED DELAYS

Contractor acknowledges that the State may not be able to meet the time frames specified in an IMS or that the State may determine that it is necessary to delay and/or modify the timing and sequencing of the implementation as provided in the IMS. While the State is committed to the project and shall use reasonable efforts to provide staff and resources necessary to satisfy all such time frames, the State shall not be held responsible or deemed in default for any delays in Solution implementation provided the State uses its reasonable efforts to accomplish its designated responsibilities and obligations as set forth in the IMS. In addition, the State may, at its option, delay implementation and installation of the Solution, or any part thereof. Notwithstanding any provision to the contrary, if the State Significantly Delays implementation of the Solution, either party may make a Change Request in accordance with Section 8, "Change Order Process," and, if required, an amendment to this Contract. Contractor agrees to adjust the IMS and Payment Milestones to take into account any State-caused delays; provided, however, that Contractor shall continue to perform any and all activities not affected by such State-caused delay. In the event the State's adjustment to the IMS causes Contractor scheduling conflicts or personnel unavailability, the State and Contractor shall prepare a revised mutually agreeable IMS which may delay the commencement and completion dates of the project and shall take into consideration the readjusted time frames and any necessary resequencing of the activities. Such readjustment, rescheduling or modification of the Project shall be at no additional cost to the State if the delays are less than or equal to thirty (30) days.

For purposes of this Section, a "Significant Delay" shall mean any delay that in itself will cause a slippage of thirty (30) calendar days or more in a Go Live date.

5.4 THIRD PARTY RESOURCES

From time to time State may request that Contractor obtain and provide to the State, at the State's expense, third party Resources related to the Services but outside the scope of what Contractor is then obligated to provide hereunder, including the benefit of any volume purchasing discounts, pricing or terms available to the State or its supplier. Contractor shall notify the State at the time of any such request of any relationships Contractor may have with such suppliers that may be of benefit to the State in this respect. To the extent that State may have a more favorable relationship with any third party supplier, upon notice

from State, Contractor agrees to consider such Resources from State's designated supplier. Contractor will not add an administrative fee or other markup to any third party Resources it procures on behalf of or for the benefit of State and the Services provided hereunder.

5.5 STATE THIRD PARTY SOFTWARE

A list of all Third Party Software licensed by the State for purposes of Contractor's performance of the Services is attached to this Attachment A as Exhibit 4. Contractor will assume operational and financial responsibility for such Third Party Software and any related maintenance obligations to the same extent as if Contractor were the licensee of such Third Party Software. Contractor will cease use of such Third Party Software upon expiration or termination of this Contract.

6. ACCEPTANCE

6.1 ACCEPTANCE TESTING BY THE STATE FOLLOWING IMPLEMENTATION

After Contractor provides written notice to the State that it has completed a phase of the solution, the State shall, in accordance with the Deliverable Expectation Document (DED) agreed by the parties, and with full cooperation and assistance from Contractor, conduct all such inspections and tests of the phase as the State may deem necessary or appropriate to determine whether any defects exist in the phase as implemented and whether the phase as installed materially complies with all of the test cases and phase specifications as set forth in the Requirements Traceability Matrix and detailed IMS. Such inspections and tests shall be over a duration mutually agreed upon by the State and Contractor, per phase, from the date a notice of completion is issued (the "Acceptance Period"). Acceptance period is defined by ten (10) business days. Contractor shall correct all defects during the Acceptance Period, demonstrate to the State that correction of such defects has been made, and after so demonstrating correction, shall issue to the State a written Deliverable Acceptance Form (DAF) indicating that no defects are known to exist in the phase and/or solution. The State shall be deemed to have accepted and approved the particular phase or solution only upon the State's delivery to Contractor of a signed, written Deliverable Acceptance Form (DAF)indicating that the phase or the solution, as the case may be, as completed, materially performs in accordance with the requirements.

If at the end of the Acceptance Period, the State has not issued a signed Deliverable Acceptance Form (DAF)to Contractor for that phase or the solution, the State may, in its sole discretion, extend the Acceptance Period; provided, however, that the State shall respond within five (5) business days of a written request by Contractor issued after the end of the original Acceptance Period to provide Contractor with the State's status of approval or disapproval for that phase or the solution. Any rejection must be in writing and specify the reason for the rejection and must be based upon the continued existence of a defect in the phase or solution or failure of the phase or solution to materially perform in accordance with the requirements. The Deliverable Acceptance Form (DAF)shall not be unreasonably withheld by the State. If a Certificate of Acceptance for a phase or the solution is signed and delivered by the State, Contractor shall sign said form, with both parties receiving a copy thereof.

7. THIRD PARTY COOPERATION

The State may hire other independent contractors as it may required to assist with the project. Contractor will cooperate with the State and the third party, including provision of: (i) written Documentation requested by the State; (ii) commercially reasonable assistance and support services to such third party; and (iii) reasonable access to Contractor as necessary for such third parties to perform their work. The State shall require such third parties to comply with Contractor's reasonable requirements regarding confidentiality, operations, standards, and security. Contractor shall support and maintain such third party

work product, provided the service provider complies with any Documentation applicable to Contractor in respect of the Services involved.

8. CONTRACT/PROJECT CHANGE ORDER PROCESS

For projects involving IT Implementation services, where frequent and/or multiple minor changes to the project schedule or deliverables are anticipated, the following process may be utilized to effectuate such minor changes without undue project delays ("Change Orders").

Changes to a Contract during its term may incur additional costs and possible delays relative to the project schedule, or may result in less cost to the State (for example, the State decides it no longer needs a deliverable in whole or part) or less effort on the part of a selected vendor. A Change Order shall define the effort involved in implementing the change, the total cost or associated savings to the State, of implementing the change, and the effect, if any, of implementing the change on the project schedule.

Any change that alters the essential terms of the original contract, including any change that expands or decreases the statement of work, the contract duration, the payment terms and/or the contract maximum amount, shall require a Contract Amendment in accordance with State contracting policies and procedures. Under no circumstances may a Change Order be used where a Contract Amendment is otherwise required pursuant to the Contract Amendments, Approval and Execution process set forth in State Administrative Bulletin 3.5.

Change Orders will be developed jointly and every effort will be made to adhere to the approved Project Plan. The Project Manager for the State and the Project Manager for a Contractor will decide whether a Change Order is necessary. If a Change Order is necessary, the Project Manager for requesting party will prepare a Change Order Request detailing the impacts on scope, schedule, deliverables, resources, and cost. The Change Order Request must be submitted to the non-requesting party for review. The non-requesting party will make its best efforts to either approve or deny the Change Order in writing within (10) business days. In no event shall any delay in the approval or denial of a Change Request constitute a deemed approval by the State.

The State will not pay for the effort involved in developing a Change Order. The Contractor shall bear the cost of estimating the cost or savings, time, and Contractor resources required to implement all Change Order Requests forthcoming from the State during the course of the Project.

All Change Orders must:

a. be in writing and describe, with specific reference to the applicable section(s) of the contract, what is being added, deleted or otherwise modified;
b. be signed by both the State and the Contractor;
c. include the original contract number and a sequential Change Order number;
d. include Contractor certifications regarding Taxes, Debarment, and Child Support, as detailed in State Administrative Bulletin 3.5, Section XIII(A)(c); and
e. be consolidated into a formal Contract Amendment whenever an amendment would otherwise be required by State Administrative Bulletin 3.5.

EXHIBIT 1
State Technical and Functional Requirements

Functional Requirements:

Data Registration and Submission Management	
F-001	Provide feedback and technical assistance to data submitters on data completeness and quality, including processing resubmitted data files, etc.
F-002	Provide a list of individuals registered to the GMCB, including payers with enrollment below the VHCURES threshold for mandated reporting of eligibility and claims data.
F-003	Maintain a method for direct communication with all registering entities and those submitting data to support notifications related to the program. Provide an overview and samples of its communication processes for both scenarios, note regular communication methods and those for changes/modifications.
F-004	Provide data summary reports to data submitters that demonstrate the data received matched the parameters that were expected, as defined by the submitter's metadata. Data summary reports provided and archived for every instance of routine submission of data and archived.
F-005	Able to collect all the required data elements established by the GMCB. Onpoint will work the GMCB, as needed, to collect additional data elements. Depending on the scope of the work, a cost proposal will be provided.
F-006	Collaborate with the State in compliance monitoring of payers with respect to registration requirements. Regularly monitor and comply with all state statutes.
F-007	Maintain documentation of data submissions, including requests for resubmissions, as well as responses to those requests. This documentation shall be made available to GMCB upon request. In addition, Outline the process and artifacts that will be provided to list out notable modifications such as fields removed, fields added, fields with substantial changes to the data submitted significant and/or low increases, additional flags that are added, etc.
F-008	Provide a data validation report to data submitters. Log the summary of data submitter for verification of data accuracy. Test and fully document during the UAT.
F-009	Conduct an annual and ongoing registration process with payers that provide coverage for Vermont residents on their enrollment. Support data submissions during the registration process and all other processes required by the State between the Vendor and the payers.
F-010	Hold one-on-one meetings and provide direct training and support to ensure that newly identified data submitters are provided with support and training to introduce the mechanics of the data submission process and expectations for data quality. Support group technical training sessions with data submitters for initial system implementation and as requested by the State when system requirements change.
F-011	Test and verify the proposed data submission processes with each data submitter prior to the submission of test data from data submitters.
F-012	Develop and maintain materials to support data submissions including examples of how to resolve common problems or errors.
Core Data Consolidation Services	
F-013	Groupers and Flags. Onpoint will provide chronic condition flags and implement risk and episode of care groupers as specified by the State. Any associated licensing fees will be covered by the State.

F-014	Measures. The State will select and implement measures in collaboration with Onpoint which may include HEDIS measures, PQA measure, readmission measure and/or Total Cost of Care metrics. If additional measures must be added at a later time, a cost proposal may be required.
F-015	Mapping and GIS coding, report generation and data visualization will be made available to the State through the Tableau BI tool.
F-016	Develop a comprehensive data quality assurance plan as part of the Data Management Plan deliverable, to be approved by the State.
F-017	Identify and document methods for incorporating claims across multiple payer types.
F-018	Maintain reference data values that are customized by payer.
F-019	Accommodate new data fields derived from existing data fields, as specified by the State. Onpoint will work with GMCB to accommodate new data fields derived from existing data fields. Depending on the scope of the work, a cost proposal will be provided.
F-020	Conduct quality checks and update the database for past submission timeframes with additional data and corrected data.
F-021	Provide complete data extracts of the claims database at a minimum of a quarterly basis and ad hoc as needed, in addition to the standard quarterly processes. Onpoint will work with the GMCB to produce ad hoc extracts, as needed. Depending on the scope of the work, a cost proposal will be provided.
F-022	Support the GMCB's and other State agencies' full access to the extracted data within the operational data set including raw, as-submitted values as requested for all years. In particular, access will not be impeded by Onpoint due to proprietary coding or any other business-specific reason. Act in accordance with the understanding that the State of Vermont is the primary steward of the data. There will be some configurability of value adds and standard reporting based on the GMCB's preferences.
F-023	Cooperate with other vendors as needed to determine data layouts and transmittal methods.
F-024	If the State develops an enterprise-wide master person index, in cases of disagreement, the default layouts and methods will be those of the data management vendor. Collaborate in developing specifications for the unique person identifier and for evaluating the accuracy of the identifier. Depending on the scope of the work, a cost proposal will be provided.
Standard Reports	
F-025	Provide status reports about data submission and conformance to GMCB's specifications, not less than monthly, to support GMCB oversight of non-compliant data submitters. These reports must also be provided as requested.
Technical Product Support	
F-026	Maintain a secure virtual, remote desktop, server or other portal that provides access to the data sets, including upgrades and up-to-date patches, for the duration of contract.
F-027	Participate in a State-appointed data users group and provide troubleshooting services for accessing or analyzing data.
F-028	Store consolidated data in a format that is efficiently designed for querying and optimized for multiple parameter filtering. The solution must follow best practices.
F-029	Ensure that historical datasets are archived and accessible to the analytic environment dating back to 2007. Historical data must be kept as long as technically feasible.
F-030	Incorporate claims data refreshes on a quarterly basis (or other basis depending on data submission schedule).
F-031	Create query performance benchmarks for user acceptance testing and performance monitoring, to be approved by the GMCB.

F-032	Provide both utilization metrics as well as performance metrics for all components of the solution to the GMCB staff upon request. Utilization metrics should be both identifiable and summarized to address audit trail as well as trends in user activity.
F-033	Scheduled maintenance of the Analytic Enclave (AE) will generally be performed the 3rd weekend of every month. Send maintenance reminders the week prior to maintenance occurring. Provide 7 or more days' notice for any scheduled downtime. Back-up data in the secure analytic environment daily.
Analytic Enclave (AE) User Access & Access Control	
F-034	Collaborate with GMCB staff to create and manage user roles and rights to the data.
F-035	Employ access controls to allow a variety of user profiles with role-appropriate access to retain data security. Provide full read-only access to the raw data tables (or views that mirror them) and the ability to create temporary tables.
F-036	Ensure that all planned maintenance services related to any components of the APCD solution are reviewed and approved by GMCB prior to their execution. Work with the GMCB to schedule and notify users about such events.
F-037	Maintain a comprehensive operational change management process.
F-038	For releases that require user acceptance testing, including major CDM front-end releases or reporting releases, the GMCB will have an opportunity to conduct UAT in a staging environment. Maintain a comprehensive, formal process for operational user acceptance testing before and after production.
F-039	Respond to all requests/questions within 24 hours.
F-040	At the conclusion of the contract, Onpoint will work with GMCB to develop a detailed transition plan that addresses the specific needs of the transition.
F-041	Maintain the Data Dictionary data documentation including version control numbering information to allow for tracking of all changes made over time.
F-042	Provide the State data documentation that includes comprehensive entity relationship diagrams covering, at a minimum, all extensions and linkages.
F-043	Produce and maintain a Data Dictionary (similar to a Code Book Structure) containing detailed specifications and documentation for the consolidated data sets, including description of files, tables, data elements, codes, and completeness of elements. Explicitly define and specify any derived fields or flags, including the source fields. Outline specification regarding each field/flag.
F-044	Create new datasets or datamarts to support analyses as they are identified by the State. Onpoint will work with the GMCB to develop the requirements for custom datasets/datamarts. Depending on the scope, a cost proposal will be developed.

Technical / Non-Functional Requirements:

Data Compliance	
NF-001	All data at rest and in motion is secure and encrypted in compliance with HIPAA and applicable State law.
NF-002	Compliance with all applicable CMS and HIPAA security guidelines, as well as pertinent state and federal laws and regulations.
NF-003	Compliance with HIPAA and HITECH security controls for relevant health care-based components.
NF-004	Service Provider will follow State of Vermont Security Standards, as referenced in HR Electronics Policy 11.7
NF-005	Compliance with the Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations.

NF-006	Compliance with Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidelines.
NF-007	Compliance with Federal Information Security Management Act (FISMA) of 2002.
NF-008	Compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
NF-009	Compliance with the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009.
NF-010	Self-registered users of applications will have identities verified per NIST SP 800-63-3.
NF-011	Confidential Personally Identifiable Information (PII) will be protected.
NF-012	Will not transmit or store any Personally Identifiable Information (PII) using storage publicly available, over the Internet or any wireless communication device, unless: 1) PII is "de-identified" in accordance with 45 C.F.R § 164.514(b) (2), 2) Encrypted in accordance with applicable law, including the American Recovery and Reinvestment Act of 2009 and as required by policies and procedures established by the State.
NF-013	Compliance with GMCB's Data Use Agreement with CMS, or other GMCB data acquisition agreements.
Data Center/Hosting & General Security Services	
NF-014	Data center facilities will be located in the continental United States.
NF-015	System availability will be 99.9% except for scheduled maintenance.
NF-016	Annual testing of the Information Security Incident Response Plan (ISIRP) will be conducted. CEO, CIO, or CTO executive approval is required for unscheduled testing.
NF-017	Periodically test incident response procedures under the direction of an incident commander. At the conclusion of each test, the commander will submit a gap analysis report to incident response management along with recommendations for corrective actions.
NF-018	Security assessments will be performed prior to releasing solutions into production. See contract Appendix D regarding submission of results.
NF-019	Maintain an Information Security Policy which describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices. Security Includes governing principles, e.g., need to know, Least Privilege, and Separation of Duties. Employees, Service Providers and temporary employees are subject to the Information Security Policy.
NF-020	Upon termination of services, provide the State with an attestation of data destruction to comply with GMCB's CMS commitment.
NF-021	Information assets will be classified in accordance with an Information Protection Policy. This policy identifies the State data as among the top two categories of confidential information, which have associated limits on access, distribution, and handling. Information will be kept confidential in accordance with security/compliance requirements.
NF-022	The State will provide a written request with information detailing the requested scope of any required audits and the regulatory obligation necessitating the audit. If a third party Service Provider is to conduct the audit, the third party Service Provider will be mutually agreed by the State and Onpoint. The third party auditor is required to

	execute a written confidentiality agreement acceptable to Onpoint before conducting the audit.
NF-023	Audits will be conducted during regular business hours, subject to policies and regulations, and will not unreasonably interfere with business activities.
NF-024	Onpoint will acknowledge that the State may be subject to audits by entities other than regulators. If the information required for such an audit is not contained in a SSAE 18 SOC 2 type 2 report, Onpoint will make reasonable efforts to provide the required information to the auditor.
NF-025	External audits against controls will be supplied to the State annually. See contract Attachment D regarding submission of results.
NF-026	Database auditing will be enabled.
NF-027	Servers will enable default log file settings for auditing critical events
NF-028	Onpoint’s data centers will regularly undergo third party auditor reviews of production deployments using the standards in the SSAE18 SOC 2 type 2. SSAE 18 require the completion of detailed testing of controls over a minimum of six months by an independent auditing body.
NF-029	OnPoint will have security and privacy requirements in its service provider contracts, which address issues such as physical and logical security requirements, privacy protection, breach reporting (See contract Attachment D) and auditing. In addition, as security requirements or services change, subcontractor contracts are changed accordingly upon renewal.
NF-030	Audits will be at the State's expense. Any request to provide assistance with an audit is considered a separate service if such audit assistance requires the use of different or additional resources beyond that used to provide the contracted services. Onpoint will seek Vermont's written approval and agreement to pay any related fees before performing such audit assistance.
NF-031	Users will be required to change their passwords to access any systems at least every 180 days.
NF-032	Integrity of the data-in-transit will be protected through the use of strong encryption (TLS/SSL or IPSec) protocols. Onpoint will configure a hashed Message Authentication Code - Secure Hash Algorithm (HMAC-SHA-1) on all IPSec VPN networks to verify that the contents of the transmission have not been altered in transit.
NF-033	Cryptographic controls will be implemented using IPSec and SSL protocols to provide end users, whether they are the State’s End Users or support engineers, with secure access to the target applications.
NF-034	Server load balancers (SLBs) with built-in SSL accelerators will be deployed in redundant pairs to offload processor-intensive SSL transactions from Servers and will be configured as a secure reverse proxy to prevent direct unmonitored access to application Servers on the public middle tier.
NF-035	Utilize a Security Information and Event Management (SIEM) system to correlate and alert on Intrusion Detection System security events, firewall log events, and network flow events. The SIEM system is monitored 24 hours per day, seven days per week, 365 days per year.
NF-036	Data Centers will contain multiple isolated network environments used to deliver Hosting Services.
NF-037	Production Environments will be isolated from Non-Production Environments.

NF-038	SSL will be used for all web-based SSL certified applications in production. Onpoint will procure SSL certificates on the State's behalf using VeriSign Corporation (or other state approved) as the Certification Authority (CA).
NF-039	Onpoint will collect and retain security evidence. A chain of custody process will be used for security incidents to maintain and document the chronological history of evidence. Each person collecting, processing, and handling evidence will record the date and time they received the evidence, and any action taken on the evidence.
NF-040	The hosting service provider shall establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. The safeguards shall provide a level of scope of security that is not less than the level and scope of security requirements established by the Office of Management and Budget in OMB circular no. A-130, appendix III, federal information processing standard 200, and special publication 800-53. Additional specifics regarding the hosting requirements are outlined in Attachment D.
NF-041	Will update and maintain an ISIRP for accuracy and effective information security incident response planning. This document will be available to Information Security Incident Response Team (ISIRT) members, systems and network administrators, information security managers, data privacy personnel, and business professionals who are responsible for preparing and responding to, information security Incidents.
NF-042	Will access state data only for the purpose of providing the services or as required by law, in accordance with the scope of services. Will not change, alter, or modify State data without State approval.
NF-043	Will monitor, alert, and protect against web application attacks of internet-facing applications. Will install, configure, and manage a web application firewall on Vermont's internet-facing Environments.
NF-044	Will monitor for, and provide alerts of, unauthorized changes to certain system and application files that would be a sign of a possible Environment compromise. As part of the service, Onpoint will perform file integrity monitoring on Vermont's servers within the ePHI Environments following the file integrity monitoring policies agreed upon by Onpoint and Vermont.
NF-045	Will require the implementation of IPSec as part of an overall VPN strategy for securing the State data between endpoints on external network connections. IPSec security associations (SAs) are configured using the IP Encapsulating Security Payload (ESP) protocol in tunneling security mode. Key exchange is accomplished through Internet Security Association Key Management Protocol (ISAKMP) using Diffie-Hellman public key techniques.
NF-046	VPN tunnel endpoints will be encrypted with (minimally) 168-bit Triple DES.
NF-047	Duration of active sessions will be limited on VPN, operating system, administrative application, and network device accounts.
NF-048	Will provide Operating System management to protect against dictionary and brute force attacks.
NF-049	The use of passwords is addressed in a Password Policy. Employees will follow rules for password length and complexity and keep their passwords confidential and secure at all times. Passwords will not be disclosed to any unauthorized person, but under certain circumstances, passwords will be communicated between authorized employees for the purpose of providing support services.

NF-050	Employees will be prohibited from altering, disabling, or removing anti-virus software and the WSUS service from any computer. Any employee who is discovered violating this standard will be subject to disciplinary action, up to and including termination.
NF-051	Will be required to install the approved full disk encryption software on their laptops, which uses a strong encryption algorithm (AES-256). Data on the disk will only be accessed through the use of a private key stored as a password protected file on the disk. A pre-boot login manager allows authorized users to login to unlock the key, boot the operating system, and access the data.
NF-052	Server Security Policy requires Windows servers to run up-to-date anti-virus software and to have SMS patch management.
NF-053	Onpoint will license and install third party Service Provider anti-virus and anti-spam products to scan all employee and the State email and inbound attachments that traverse either the State's dedicated servers located at Hosting Service Provider's Data Centers.
NF-054	Email infrastructure servers, by default, have "opportunistic encryption" using TLS, which allows encryption on both inbound and outbound emails depending on the capabilities of the State's email systems. Will enforce encryption using TLS for its emails traversing the email infrastructure.
NF-055	Servers will have operating systems hardened by eliminating unnecessary system services, accounts, network services, limited user access rights throughout the environments.
NF-056	Will evaluate and respond to Incidents that create suspicions of unauthorized access to or handling of State data, whether the data is held on Onpoint, the State, or third party Service Provider owned hardware, or on the personal hardware assets of employees and contingent workers. Onpoint will be informed of such Incidents and, depending on the nature of the activity, define escalation paths and response teams to address those Incidents. Onpoint will work with the State, internal LOB, the appropriate technical teams, and where necessary, outside law enforcement to respond to the Incident. The goal of the Incident response will be to restore the confidentiality, integrity, and availability of the State's Environment, and to establish root causes and remediation steps.
NF-057	Network device configurations will be hardened by performing the following: -Disabling telnet access. -Controlling Simple Network Management Protocol (SNMP) access to devices. -Controlling access to devices through the use of Terminal Access Controller Access Control System Plus (TACACS+). -Turn off unneeded services. - Perform appropriate level of logging.
NF-058	Environments will undergo a security assessment process that includes review of programs, hardware and operating system components. New releases are installed in a shared staging environment for final validation prior to Production Go-Live.
NF-059	Programs are deployed on a Server(s) in accordance with the Certified Configuration and/or detailed build procedures. A standard "Kick Start" image is used to install the operating system and a package manager is then used to automatically install the utility programs required for the type of Server being configured. Finally, the file system is built and Programs are installed from standard images. Hardening procedures are embedded within a Certified Configuration.

General Security	
NF-060	Certified Configuration systems will be hardened and undergo security assessments. State environments will be deployed with Certified Configurations.
NF-061	Will complete and supply to the State, CMS Security required documentation including System Security Plan (SSP), Risk Assessment (RA), and Contingency Plan (CP). Onpoint will supply its Information Security Program documentation under a non-disclosure agreement upon request.
NF-062	Data Masking is designed to obscure specific data elements and will be used in non-production databases in Vermont's ePHI Environments, by replacing actual, sensitive data identified by Vermont with false, simulated data. The objective of the service is to prevent ePHI contained in specific database fields, from being disclosed to unauthorized parties.
NF-063	Will deploy, monitor and manage third party host-based Data Loss Prevention (HDLP) software on the Windows workstations of support personnel. The HDLP software is designed to monitor DBA and system administration activity and alert for, or block, potential unauthorized access to Vermont's ePHI.
NF-064	HIPAA Security Services will require controls on desktops and laptops used to connect to ePHI environments: - Anti Virus software.- Full disk encryption.- Removable media encryption.- Host data loss prevention.
NF-065	Will provide to the State the SSAE 18 SOC 2 type 2 reports for its data centers.
NF-066	ePHI Environments will be included in HIPAA Compliance assessment performed by a qualified third party auditor, and provide Vermont with the summary information from the third party assessment report.
NF-067	Will conduct quarterly reviews of the firewall policies and network devices configurations for Vermont's ePHI Environments.
NF-068	Will conduct an annual risk assessment of ePHI environments against the HIPAA controls to ensure compliance and provide findings to Vermont.
NF-069	Will create and review a security assessment checklist to be included in Vermont's Periodic Maintenance Plan. In addition, Onpoint will review the results provided in the Base Services and include recommendations for updates, including any recommendations for remediation to any identified vulnerabilities.
NF-070	Logs with security-relevant information will be retained for three months.
NF-070	Will review logs for forensic purposes and Incidents, and any anomalous activities are incorporated into the Incident management process.
NF-072	Will log security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to the Environment or Programs, as well as system alerts, console messages, and system errors. Controls will be implemented to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Security-related log entries will capture the following information: date, time, time zone, user account name and/or IP address, original value, location of change (hostname, filename, table name), new value (other than password).
NF-073	Will provide to the State relevant Breach, Security, or Enforcement policies.
NF-074	Will maintain a Security Organization Policy describing and clarifying the roles and responsibilities of various teams and individuals involved in information security, including: -Executive-level Oversight Committee

	-Corporate Information, Product, and Physical Security organizations - IT and IT Security organizations Lines of business (LOBs) and individual Information Security Managers (ISMs) will be assigned to represent the security leadership of each organization.
NF-075	Will employ an integrated security management system with electronic photo ID badges, cardholder access control, recorded digital video surveillance, and alarm monitoring within its data centers. Data Centers will have a single entrance that is manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management. Building perimeters will use alarm systems and a 24x7 security protection unit.
NF-076	Multi-factor authentication (MFA) will be used for internal Onpoint VPN access as well as for Vermont end users to access the Vermont Analytic Enclave. Users must supply a username, password and MFA code. Users may receive the code via a MFA token. Users could also receive a push notification to their mobile device instead of providing the MFA code. Users must approve the push notification on their mobile device to gain access to the environment.
NF-077	Will conduct an annual network and application penetration test for Vermont's Production Environment and provide a report on the results of the network and application penetration test. See contract Appendix D regarding submission of results.
NF-078	Will define by department, role, and/or individual employee/user, the access levels and privilege set to create, read, update/change, or delete data. This includes definitions at the State level.
NF-079	Will log unsuccessful login attempts.
NF-080	Will provide Certificate Authority for secure server side transactions.
NF-081	Will support issue and manage public key certificates for secure transactions.
NF-082	Will ensure non-repudiation as part of digital signature verification to prevent data from being altered, deleted or damaged during exchange.
NF-083	Will set automatic alerts to system administrators when a breach pattern or unauthorized use activity is detected.
NF-084	Strong authentication will be employed in all deployment environments.
NF-085	Directories will be accessible via the LDAP protocol.
NF-086	Will support isolation within the directory for storing internal and external users.
NF-087	Database data will be encrypted at the file system layer.
NF-088	Data stored on file systems will be encrypted.
NF-089	Fraud detection functionality will be implemented.
NF-090	Access to PHI Servers will be restricted to those employees who have successfully completed HIPAA training and proof of successful completion will be available to the State upon request.
NF-091	Will support "user exits" or a "pluggable authentication module" (PAM) to enable user transition between Solutions and local systems that are authorized as third party connections to the Solution. Implementation of functionality is being evaluated. Depending on the scope of the work, a cost proposal will be provided.
NF-092	Will have the ability to assign users to multiple OMS (Organization Management System) organizations with different applications and roles.
NF-093	Will implement security for transport and messaging via web services.
NF-094	Identity Management systems will be implemented using a 'virtual directory' model to abstract directory sources and improve maintainability.

NF-095	System will be delivered with no viruses or malware.
NF-096	Ensure that security violations are identified, documented, resolved, and reported to the State.

EXHIBIT 2
Preliminary Implementation Master Schedule

Task Name	Duration	Start	Finish	Predecessors	Resource Names	Text1
VHCURES 3.0 Implementation	**266 days**	**Thu 8/15/19**	**Wed 8/26/20**			
Project Initiation	**6 days**	**Thu 8/15/19**	**Thu 8/22/19**			
VHCURES 3.0 contract execution	1 day	Thu 8/15/19	Thu 8/15/19		GMCB/Onpoint	
VHCURES 3.0 kick-off meeting	5 days	Fri 8/16/19	Thu 8/22/19	3	Onpoint/GMCB	
Project Management	**260 days**	**Fri 8/23/19**	**Wed 8/26/20**			
Project management plan development	10 days	Fri 8/23/19	Fri 9/6/19	4	Onpoint	
Weekly project meetings	13 mons	Fri 8/23/19	Wed 8/26/20	4	Onpoint/GMCB	
Quarterly in-person meetings	13 mons	Fri 8/23/19	Wed 8/26/20	4	Onpoint/GMCB	
Change management plan development	30 days	Fri 8/23/19	Fri 10/4/19	4	Onpoint	
Data quality plan development	30 days	Fri 8/23/19	Fri 10/4/19	4	Onpoint	
VHCURES 2019 Quarterly Extract Production	**301 days**	**Mon 9/30/19**	**Wed 7/29/20**			
Paid through June 2019 (2019Q2) extract production	30 days	Mon 9/30/19	Tue 10/29/19		Onpoint	2019Q1 Medicare expected 9/2019.
Paid through September 2019 (2019Q3) extract production	30 days	Tue 12/31/19	Wed 1/29/20		Onpoint	2019Q2 Medicare expected 12/2019.
Paid through December (2019Q4) production	30 days	Tue 3/31/20	Wed 4/29/20		Onpoint	2019Q3 Medicare expected 3/2020.
Paid through March 2020 (2020Q1) extract production	30 days	Tue 6/30/20	Wed 7/29/20		Onpoint	2019Q4 Medicare expected 6/2020.
New Analytic Tools Implementation	**202 days**	**Fri 8/16/19**	**Fri 5/29/20**			
Service Line Flagging Implementation	**52 days**	**Fri 8/16/19**	**Tue 10/29/19**			
Overview of SL flags provided to the GMCB	5 days	Fri 8/16/19	Thu 8/22/19	4FF	Onpoint/GMCB	
SL flags configuration	1 day	Fri 8/23/19	Fri 8/23/19	18	Onpoint	
SL flags quality review and remediation	5 days	Mon 8/26/19	Fri 8/30/19	19	Onpoint	
SL flags delivery (2019Q2 extract)	0 days	Tue 10/29/19	Tue 10/29/19	12	Onpoint	
Documentation updates	30 days	Wed 9/18/19	Tue 10/29/19	21FF	Onpoint	
Chronic Condition Flags Implementation	**130 days**	**Fri 8/16/19**	**Wed 2/19/20**			
Overview of CC flags provided to the GMCB	5 days	Fri 8/16/19	Thu 8/22/19	4FF	Onpoint/GMCB	
CC flags selection by the GMCB	5 days	Fri 8/23/19	Thu 8/29/19	24	GMCB/Onpoint	
CC flags configuration	5 days	Fri 8/30/19	Fri 9/6/19	25	Onpoint	
CC flags production (2019Q3 extract)	10 days	Thu 1/30/20	Wed 2/12/20	13	Onpoint	
CC flags quality review and remediation	5 days	Thu 2/13/20	Wed 2/19/20	27	Onpoint	
CC flags available for the PLR	0 days	Wed 2/19/20	Wed 2/19/20	28	Onpoint	
Documentation updates	30 days	Thu 1/9/20	Wed 2/19/20	29FF	Onpoint	
Measures Implementation	**130 days**	**Fri 8/16/19**	**Wed 2/19/20**			
Overview of measures provided to the GMCB	5 days	Fri 8/16/19	Thu 8/22/19	4FF	Onpoint/GMCB	
Measures selection by the GMCB	5 days	Fri 8/23/19	Thu 8/29/19	32	GMCB/Onpoint	
Measures configuration	5 days	Fri 8/30/19	Fri 9/6/19	33	Onpoint	
Measures production (2019Q3 extract)	10 days	Thu 1/30/20	Wed 2/12/20	13	Onpoint	
Measures quality review and remediation	5 days	Thu 2/13/20	Wed 2/19/20	35	Onpoint	
Measures available for the PLR	0 days	Wed 2/19/20	Wed 2/19/20	36	Onpoint	
Documentation updates	30 days	Thu 1/9/20	Wed 2/19/20	37FF	Onpoint	
Risk Classification Implementation	**130 days**	**Fri 8/16/19**	**Wed 2/19/20**			
Grouper licensing executed	5 days	Fri 8/16/19	Thu 8/22/19	3	Onpoint/GMCB	
Overview of grouper provided to the GMCB	5 days	Fri 8/16/19	Thu 8/22/19	4FF	Onpoint/GMCB	
Grouper configuration	5 days	Fri 8/23/19	Thu 8/29/19	41	Onpoint	
Grouper production (2019Q3 extract)	10 days	Thu 1/30/20	Wed 2/12/20	13	Onpoint	
Grouper quality review and remediation	5 days	Thu 2/13/20	Wed 2/19/20	43	Onpoint	
Grouper available for the PLR	0 days	Wed 2/19/20	Wed 2/19/20	44	Onpoint	
Documentation updates	30 days	Thu 1/9/20	Wed 2/19/20	45FF	Onpoint	
Episode of Care (EOC) Grouper Implementation	**202 days**	**Fri 8/16/19**	**Fri 5/29/20**			

Page 1

Task Name	Duration	Start	Finish	Predecessors	Resource Names	Text1
Overview of EOC grouper provided to the GMCB	5 days	Fri 8/16/19	Thu 8/22/19	4FF	Onpoint/GMCB	
EOC services selected by the GMCB	5 days	Fri 8/23/19	Thu 8/29/19	48	GMCB/Onpoint	
EOC grouper configuration	90 days	Fri 8/30/19	Wed 1/8/20	49	Onpoint	
EOC grouper production (2019Q4 extract)	10 days	Thu 4/30/20	Wed 5/13/20	14	Onpoint	
EOC grouper quality review and remediation	10 days	Thu 5/14/20	Wed 5/27/20	51	Onpoint	
EOC grouper delivery (Q4 extract)	2 days	Thu 5/28/20	Fri 5/29/20	52	Onpoint	
Documentation updates	30 days	Mon 4/20/20	Fri 5/29/20	53FF	Onpoint	
Patient-to-Provider Attribution Implementation	**130 days**	**Fri 8/16/19**	**Wed 2/19/20**			
Overview of attribution provided to the GMCB	5 days	Fri 8/16/19	Thu 8/22/19	4FF	Onpoint/GMCB	
Attribution configuration selected by the GMCB	5 days	Fri 8/23/19	Thu 8/29/19	56	GMCB/Onpoint	
Attribution configuration	5 days	Fri 8/30/19	Fri 9/6/19	57	Onpoint	
Attribution production (Q3 extract)	5 days	Thu 1/30/20	Wed 2/5/20	13	Onpoint	
Attribution quality review and remediation	10 days	Thu 2/6/20	Wed 2/19/20	59	Onpoint	
Attribution available for the PLR	0 days	Wed 2/19/20	Wed 2/19/20	60	Onpoint	
Documentation updates	30 days	Thu 1/9/20	Wed 2/19/20	61FF	Onpoint	
Person-Level Report (PLR) Implementation	**133 days**	**Fri 8/23/19**	**Mon 3/2/20**			
Overview of the PLR provided to the GMCB	5 days	Fri 8/23/19	Thu 8/29/19	4	Onpoint/GMCB	
PLR Requirements	5 days	Fri 8/30/19	Fri 9/6/19	64	Onpoint/GMCB	
PLR development	10 days	Mon 9/9/19	Fri 9/20/19	65	Onpoint	
PLR production	3 days	Thu 2/20/20	Mon 2/24/20	37,45,61,29	Onpoint	
PLR quality review	5 days	Tue 2/25/20	Mon 3/2/20	67	Onpoint	
PLR delivery	0 days	Mon 3/2/20	Mon 3/2/20	68	Onpoint	
PLR Documentation updates	30 days	Tue 1/21/20	Mon 3/2/20	69FF	Onpoint	
Member Year (MY) Table Implementation	**115 days**	**Fri 8/16/19**	**Wed 1/29/20**			
Overview of MY table provided to the GMCB	5 days	Fri 8/16/19	Thu 8/22/19	4FF	Onpoint/GMCB	
MY table configured	5 days	Fri 8/23/19	Thu 8/29/19	72	Onpoint	
MY table quality review	5 days	Fri 8/30/19	Fri 9/6/19	73	Onpoint	
MY table production (2019Q3 extract)	30 days	Thu 12/19/19	Wed 1/29/20	13FF,74	Onpoint	
MY table delivery (2019Q3 extract)	1 day	Wed 1/29/20	Wed 1/29/20	13FF	Onpoint	
Documentation updates	30 days	Thu 12/19/19	Wed 1/29/20	13FF	Onpoint	
Analytic File (AF) Implementation	**82 days**	**Fri 8/16/19**	**Fri 12/13/19**			
AF production schedule reviewed with the GMCB	5 days	Fri 8/16/19	Thu 8/22/19	4FF	Onpoint/GMCB	
AF production	20 days	Wed 10/30/19	Wed 11/27/19	12	Onpoint	
AF quality review	5 days	Mon 12/2/19	Fri 12/6/19	80	Onpoint	
AF delivered	5 days	Mon 12/9/19	Fri 12/13/19	81	Onpoint	
Documentation updates	30 days	Wed 10/30/19	Fri 12/13/19	82FF	Onpoint	
Analytic Enclave (AE) and Tableau Setup	**260 days**	**Fri 8/23/19**	**Wed 8/26/20**			
Requirements	2 wks	Fri 8/23/19	Fri 9/6/19	4	Onpoint/GMCB	
New AE Seats Implementation	**60 days**	**Fri 8/23/19**	**Mon 11/18/19**	**4**		
New AWS Workspaces setup for new users	60 days	Fri 8/23/19	Mon 11/18/19		Onpoint	
Role-based and user-based access to the Redshift database	60 days	Fri 8/23/19	Mon 11/18/19		Onpoint	
Installation of analytic tools	60 days	Fri 8/23/19	Mon 11/18/19		Onpoint	
User Training	60 days	Fri 8/23/19	Mon 11/18/19		Onpoint	
Tableau Installation and Configuration	**190 days**	**Mon 9/9/19**	**Wed 6/3/20**			
Overview of licensing options provided to the GMCB	5 days	Mon 9/9/19	Fri 9/13/19		Onpoint/GMCB	
Licensing selection by the GMCB	15 days	Mon 9/16/19	Fri 10/4/19	92	GMCB/Onpoint	

Page 2

Task Name	Duration	Start	Finish	Predecessors	Resource Names
Tableau license procurement	2 wks	Mon 10/7/19	Fri 10/18/19	93	
Tableau Server installation and configuration	2 wks	Mon 10/21/19	Fri 11/1/19	94	Onpoint
Tableau Desktop installation and configuration in AE	2 wks	Mon 10/21/19	Fri 11/1/19	94	Onpoint
Tableau setup and configuration testing	2 wks	Mon 11/4/19	Mon 11/18/19	95	Onpoint
GMCB UAT of Tableau Server	2 wks	Tue 11/19/19	Wed 12/4/19	97	GMCB
Remediation	2 wks	Thu 12/5/19	Wed 12/18/19	98	Onpoint
Documentation	1 wk	Thu 12/19/19	Wed 12/25/19	99	Onpoint
Release to production	1 day	Thu 12/26/19	Thu 12/26/19	100	Onpoint
BI Standard Reports	**130 days**	**Thu 12/5/19**	**Wed 6/3/20**		
Overview of standard reports provided to the GMCB	2 wks	Thu 12/5/19	Wed 12/18/19	33SS+70 days,25	Onpoint/GMCB
Standard reports selected with the GMCB	2 wks	Thu 12/19/19	Wed 1/1/20	103	GMCB
Configuration	2 wks	Thu 1/2/20	Wed 1/15/20	104	Onpoint
Development of data model and standard reports based on measures, chronic conditions, and report selections	10 wks	Thu 1/16/20	Wed 3/25/20	105	Onpoint
Onpoint Testing and remediation	4 wks	Thu 3/26/20	Wed 4/22/20	106	Onpoint
GMCB testing and remediation	4 wks	Thu 4/23/20	Wed 5/20/20	107	GMCB
Release to Production	5 days	Thu 5/21/20	Wed 5/27/20	108	Onpoint
Documentation	2 wks	Thu 4/23/20	Wed 5/6/20	107	Onpoint
Client Training	1 wk	Thu 5/28/20	Wed 6/3/20	109	Onpoint/GMCB
Project Close - VHCURES 3.0 Implementation	**60 days**	**Thu 6/4/20**	**Wed 8/26/20**		
Lessons learned sessions	30 days	Thu 6/4/20	Wed 7/15/20	111	Onpoint/GMCB
Finalize documentation	30 days	Thu 7/16/20	Wed 8/26/20	113	Onpoint

EXHIBIT 3
Operational Tasks/Payment Schedules

Background

The Green Mountain Care Board (GMCB) is the steward of several data resources. In this role, the GMCB is responsible for a broad set of data management and stewardship concerns. The data may be used in analysis by agencies and academic researchers interested in questions, such as access to care, expenditures, utilization, and quality.

The Vermont Health Care Uniform Reporting and Evaluation System (VHCURES) is the State's all-payer claims database. The VHCURES database includes eligibility information and medical and pharmacy claims provided by commercial health insurers as well as Medicaid and Medicare beginning in January 2007. Through data use agreements, VHCURES data is utilized by state agencies, state and federal contractors, and other approved users to support analysis of health care access, spending, utilization, and quality.

The GMCB envisions a more robust, performant solution that improves the consistency of access, including recurring reports produced by the vendor. Increasing the use of the data resource should also help improve the quality of the data and subsequent analysis. The GMCB will continue to use the data to supports its regulatory duties and inform efforts as guided by the Vermont Legislature.

The State released a Request for Proposals in September 2018 for an independent, third-party vendor to enhance the State's existing all-payer claims database.

The State will provide direction to the Contractor to assume work under this contract. Work may be performed at the Contractor's office location, regular phone calls will be required, with the possibility of in-person meetings.

State of Vermont Key Personnel for Contract #38739:

- David Glavin, Data and Reporting Project Manager, GMCB – Operations Contract Manager
- Sarah Lindberg, Health Services Researcher, GMCB – Subject Matter Expert, Data and Analytics
- Kate Carter, Enterprise IT Project Manager, Agency of Digital Services – Implementation Project Manager and Vendor Manager

The State will notify the contractor of any personnel changes in writing within 30 days and will file changes to the contract file.

Data Aggregation
Task 1: Registration and Data Submission

1.1 *Registration Requirements and Collection of Information*:

- Access
  - Provide web-based and secure access to an online system that supports State registration requirements and collection of information for mandated health insurers and related parties (e.g. TPAs, PBMs).
- Communication
  - Maintain a method for direct communication with all registering entities and the submissions of those submitting data to support notifications related to the program.
- Notification
  - Provide notifications to all registrants and submitters on program updates, annual registration reminders, required downtime, changes/modifications to data submission specifications, and notifications of upcoming webinars or training sessions. Notification for annual registration will be issued 30 days prior to date registration opens.
- Registry of Contact Information
  - Maintain contact information registry, updated annually for all registrants, for use by the Contractor and the State with adequate detail including company names, company registration or registration codes, company contacts and titles, mailing and email addresses, and telephone numbers for all registered entities and data submitters.
  - Update the registry if registrants provide new or replacement information outside the annual registration period.
- Compliance Monitoring
  - Collaborate with the State in compliance monitoring of payers with respect to registrations requirements.
  - Regularly monitor and comply with all state statutes.

1.2 *Registration*:

Conduct an annual and ongoing registration process with payers that provide coverage for Vermont residents on their enrollment. Support data submissions during the registration process and all other processes required by the State between the Vendor and the payers.

- Registration Plan
  - Collaborate with the State to develop an annual registration plan by September 1 to identify potential changes to the annual process and a timeline for implementing modifications as approved by the State.
- Deadline Notification
  - Directly notify current registrants and data submitters of each impending annual registration deadline of December 31, 60 days prior to the deadline.
  - Provide direct notification following the deadline for any registrants and data submitters that have not renewed their registration.
- Registration Access
  - Provide web-based and secure access to registration tool that supports State registration requirements and collection of information for TPAs and PBMs and registration of mandated reporters to support the data submission process; file submission instructions; reporter-specific secure access for on-line file submission; and access to status and error reports and other necessary information.

- Reporting
    - Provide a list of registrants to the GMCB, including payers with enrollment below the VHCURES threshold for mandated data submission of eligibility and claims data including, but not limited to active submitters, payers who have registered but do not submit, and inactive submitters. including a final, annual report submitted for GMCB's review and approval.
    - Provide the State with up-to-date data/reports by registrant that supports compliance monitoring

1.3 *Data Submission:*

- Able to collect all the required data elements established by the GMCB. Onpoint will work the GMCB, as needed, to collect additional data elements. Depending on the scope of the work, a cost proposal will be provided.
- Adhere to the change management process agreed upon with the State when data elements change.
- Recommend modifications to the data submission requirements as needed based on the most current standards for claims, eligibility and other relevant administrative health data that will support the diverse and evolving informational needs of the State.
- Provide technical assistance to the State regarding potential modifications to data submission rules and other requirements and for discussions with other entities regarding such potential modifications.
- Training and Support
    - Onboarding Newly Identified Data Submitters
        - Hold one-on-one meetings and provide direct training and support to ensure that newly identified data submitters are provided with support and training to introduce the mechanics of the data submission process and expectations for data quality. Support group technical training sessions with data submitters for initial system implementation and as requested by the State when system requirements change.
        - Test and verify the proposed data submission processes with each data submitter prior to the submission of test data from data submitters.
    - Ongoing
        - Provide secure access to feedback and technical assistance to data submitters on data completeness, validation and quality, including processing resubmitted data files.
        - Develop and maintain materials to support data submissions, including examples of how to resolve common problems or errors.
        - Support group technical training sessions with data submitters as requested by the State when system requirements change.
        - Test and verify the proposed data submission processes with each data submitter prior to the submission of test data from data submitters.
- Reports to Data Submitters
    - Provide data summary reports to data submitters that demonstrate the data received matched the parameters that were expected, as defined by the submitter's metadata.
    - Provide a data validation report to data submitters.
- Provide and archive data summary reports for every instance of routine submission of data.
- Log the summary of data submitter for verification of data accuracy. In addition, test and fully document during the User Acceptance Testing (UAT).

- Provide access to data and reports related to file submission, status, exceptions to thresholds and other relevant information pertaining to data submission compliance.
    - Maintain documentation of data submissions, including requests for resubmissions, as well as responses to those requests and make available to GMCB upon request.
    - Provide GMCB documentation of notable modifications including, but not limited to:
        - Fields removed
        - Fields added
        - Fields with substantial changes to the data submitted significant and/or low increases
        - Additional flags that are added.

Task 2: Claims Data Collection and Consolidation Services:

Update Onpoint CDM edits for Vermont reporters to include recommended data revisions and transitional planning.

Daily processing of live data, including new and resubmitted data, noncompliance notification, and transitional planning as required.

- Collect medical claims, pharmacy claims, eligibility data, and other related data files from mandated and voluntary data submitters as referenced in applicable rules and regulations of the State of Vermont. Data submitters will include commercial health insurers, third-party administrators, pharmacy benefit managers, Medicaid, and Medicare.
- Provide registered submitters with secure access for online file submission; and access to status reports, error reports, and other necessary information.
- Provide technical assistance to new data submitters as well as established data submitters as needed to support efficient, accurate, and timely data submission and other requirements as directed by the State.
- Make a reasonable effort to accommodate data transfer methods preferred by data submitters while maintaining optimal security standards.
- Meet security standards for Medicare data containing direct identifiers as specified in Section 7 of the CMS Data Use Agreement Form CMS-R-0235 as the State's (CMS licensee) designated custodian (CMS custodian).
- Retain fields and data elements unique to Commercial, Medicaid, and Medicare that will support analytical capability of both the integrated all-payer data set and also stand-alone files for each payer type including Commercial, Medicaid, and Medicare. Covered populations will include comprehensive major medical insureds, Medicare Supplemental insurance beneficiaries, and Medicare Parts C and D beneficiaries.
- Collect and integrate files from the Centers for Medicare and Medicaid Services (CMS) provided to the State as the licensee and the Contractor as custodian.
- Integrate the following Medicare standard formats into VHCURES using the layout as defined by Vermont Regulation H-2008-01: Standard quarterly Research Identifiable (RIF) and Medicare Part D event files.
    - Standard RIF files will include eligibility and Medicare Part A and Part B files and an annual refresh file.
- Submitted File Evaluation. Evaluate submitted files for conformance to the file layout, format and metadata included in header and trailer records to ensure that submitted data satisfies basic requirements and is viable to proceed with processing. This evaluation step will include, but is not limited to, verifying satisfaction of the following conditions:
    - The file contains only one header record and one trailer record, both of which are formatted correctly

  - The file is in the proper format as specified by the State
  - The correct number of fields appears in each record
  - The number of data records matches the count reported in the header record
  - Data types and lengths are valid
  - Applicable dates within the file are within the reporting period beginning and period ending values cited in the header and trailer records
  - Data that is required to be hashed is hashed
- If data files conform to their metadata descriptions, and otherwise appear to be valid files, then the Contractor will proceed with processing the files.
- In the event transmitted files fail this evaluation, then Onpoint will provide such notification to the data submitter and apply best efforts to support the resubmission of valid files.
- For each received submission point will maintain:
  - Retrievable records of the dates on which files were received
  - Results of the evaluation, and
  - Other pertinent information to document the acquisition of files.
- Data Evaluation: For data files that meet passable standards for data receipt, conduct an evaluation of the content of these files for soundness, completeness, and reasonableness. The evaluation will include, but not be limited to, verifying satisfaction of the following conditions:
  - Data is accurately formatted
  - The prevalence of null or missing data is below threshold levels
  - Values supplied for specific fields are logical
  - Codes are appropriately used
  - Data elements have appropriate interrelationships
  - Tolerance levels as reviewed and collaborated upon with the State on an annual basis.
  - For files that fail to meet these evaluation steps, Onpoint will provide such notification and suitable explanation to the data submitter and, if requested, to the State.
  - Onpoint will apply best efforts to support the resubmission of accurate files.
  - Onpoint will maintain retrievable records of the results of the evaluation of the content of data files.
- Work with all submitters and recipients of data to ensure that protected health information (PHI) is protected both in transmit and at rest and that the data is hashed and/or encrypted for secure transmission. When PGP encryption is used, Onpoint will work with the other party in sharing encryption keys at no cost and testing the process.
- Identify and document methods for incorporating claims across multiple payer types including one for each payer type and one for each file type.
- Integrate historical data already residing in the VHCURES consolidated database (from first service dates of January 1, 2007 onward) and continue to collect the required claims, eligibility and other related data files already residing in VHCURES, integrating commercial, Medicaid and Medicare data.
- Perform provider linkage to support the maintenance of a VHCURES provider database and a Master Provider Index (MPI) to facilitate the following:
  - Accurate attribution of claims records to single providers or provider groups;
  - Aggregation of claims for single provider or groups of providers with the same specialty code;
  - Attribution of members to single providers and provider groups that can be further categorized by specialty code type such as primary care and other specialty types; and
  - Attribution of providers to injury/illness types.
- Perform provider linkage to resolve provider identity with their unique NPI number.
- Groupers and Flags. Onpoint will provide chronic condition flags and implement risk and episode of care groupers as specified by the State. Any associated licensing fees will be covered

by the State.

- Measures. The State will select and implement measures in collaboration with Onpoint which may include HEDIS measures, PQA measure, readmission measure and/or Total Cost of Care metrics. If additional measures must be added at a later time, a cost proposal may be required.
- Mapping and GIS coding, report generation and data visualization will be made available to the State through the Tableau BI tool.

2.1 *Data Quality Assurance Plan*

Develop a comprehensive Data Quality Assurance Plan to be incorporated in the Delivery Expectation Document (DED).

- The comprehensive data quality assurance plan will include, but not limited to the following metrics:
  - completeness and validity
  - element relationships
  - trending and cross-file quality
  - submitter attestation on an annual basis for the submitters making up 80% of the claims volume
  - cross-payer validation
  - quality
  - utilization, and
  - expenditure metrics

- On a quarterly basis, conduct an evaluation of the trends implied by the files in the context of the data historically provided by their respective submitters, as well as in the context of industry accepted standards for such trends. Relevant aspects of the data to be trended shall include, but not be limited to:
  - Total medical claims counts
  - Total pharmacy claims counts
  - Total dollar value of medical claims
  - Total dollar value of pharmacy claims
  - Total eligibility counts
  - Total orphan claims
  - Per member per month medical claims cost
  - Per member per month pharmacy claims cost

- For each data submitter, these trends shall be rendered by product, and shall reflect three years of that submitter's data. If three years of data is not available, then the trends shall encompass as much of the submitter's data as is available.
- Data points for the above criteria shall be provided by month. For data files that show anomalies in trends, Onpoint will put forth best efforts to understand the causality of such discrepancies and collaborate with the State and the data submitter to determine the most suitable approach to resolution.
- Records of these trend analyses will be maintained in a retrievable manner, and made available to the State.
- Conduct quality checks and update database for past submission timeframes with additional data and corrected data.
- Consult with the State regarding the approach and methods that are used to generate unique identifiers for individual persons (i.e., patients, members, enrollees, beneficiaries) to support

assignment of claims to individuals within and across insurers and payers within the VHCURES data set.

- Maintain reference data values that are customized by payer. Map the specific reference tables and to payer-specific and standard codes to the payer and be consistent across the database and implemented for the entirety of the contract.

Task 3: Data Access, Management, and Support

- Contractor shall provide copies to the State of a standardized comprehensive data extract generated from the VHCURES data warehouse at no additional cost (other than those outlined in Table 4). Incorporate claims data refreshes on a quarterly basis (or other basis depending on data submission schedule) and be subject to a mutually agreed upon DED and DAF.

- Copies of the standard state agency quarterly extract will also be generated at no additional cost for Vermont state agencies with VHCURES data use agreements and their contractors and researchers who are performing State-directed work. Contractor may bill approved users that are not Vermont State agencies or authorized State contractors for the staff time required to prepare, ship, or transmit extracts.

- At the time of execution of this contract, these charges for non-Vermont state agencies and contractors are $5,250 with no changes to the table layout. This pricing assumes delivery via SFTP or to the Vermont Analytic Enclave. There is a one-time fee of $550 for initial SFTP set-up and testing. An estimate will be provided if hard media is requested. These charges for non-Vermont state agencies and contractors are subject to change over time.

- In cases where data linkage is approved by the GMCB, Onpoint shall provide encryption keys or other necessary elements at no cost to allow an authorized user to perform linkage. Onpoint can charge an approved user if Onpoint is conducting the linkage on behalf of the approved user.

- Contractor will provide the VT Analytic File, a simplified extract consisting of five (5) core tables, annually to the GMCB. The VT Analytic File will be run on calendar year data with three (3) months of paid run-out. For deliveries outside of the Analytic Enclave or the GMCB SFTP system there is a one-time fee of $550 for initial SFTP set-up and testing.

- Provide a secure, cloud-based analytic enclave to State approved users.

- Vulnerability Testing. Onpoint shall run (or prove evidence of having been run) quarterly vulnerability assessments on externally facing assets storing or presenting state data including hosted or on premises infrastructure. Results will be delivered quarterly to the ADS security team, or technical lead for the program. Contractor shall remediate all critical/high issues within 90 days. Contractor shall provide a risk mitigation plan for medium and low issues. Contractor shall obtain written State approval for any exceptions. Contractor will work with the state to define a reporting process.

  Onpoint will provide a copy of its HITRUST certification letter, HITRUST executive summary report, and annual penetration testing, annually, upon request.

- *Pricing:* User subscription pricing is included in Table 4 for 26-30 seats in the Analytic Enclave (AE) at $12,000 per month. There is a minimum of five (5) users required per Analytic Enclave

subscription. Contractor cannot support shared user accounts or concurrent users in the Analytic Enclave. Additional seats will be priced according to the following schedule:

Number of Seat	Analytic Enclave pricing, total cost per month
6	$6,050
7	$6,725
8	$7,400
9	$7,400
10	$7,400
11 to 15	$9,000
16 to 20	$10,250
21 to 25	$11,250
26 to 30	$12,000

The baseline RedShift size is 2 terabytes. If the client requires additional space, Onpoint can provision additional nodes. Each incremental node provides an additional 2 terabytes at a cost of $600 per month.

- Users within the Analytic Enclave can be provided access to Tableau Creator at GMCB's request. If GMCB does not have an existing Tableau license that can be utilized, then Contractor can purchase Tableau licenses with a one-year commitment. Tableau's pricing is subject to change and Onpoint agrees to only pass direct Tableau cost to GMCB with no additional fees.

- If more than 250GB of storage space per user is required, the additional space will be charged at $34.50 per 100GB per month (includes 14-day retention of backups).

- Changes to approved users will be communicated to Onpoint according to a mutually agreed upon procedure.

- Provision new users in the Analytic Enclave within two business days of request, with an active start date relative to monthly access. Multiple new users at the same time would require additional time, so, for example, 10 days would be required for 5 new users requested on the same day. 3 business days are required for an AE seat termination. Onpoint will accommodate immediate terminations in the AE, as needed, for unexpected termination of employment.

- Manage all access control. Pricing assumes seats will not turn over more frequently than once every six months. The State will request support as directed in the Analytic Enclave Support document.

- The Analytic Enclave will be built out in the Amazon Web Services (AWS) cloud-based environment. The GMCB will have its own dedicated virtual private cloud (VPC). Users will connect to the Analytic Enclave using AWS workspaces. Their AWS workspace will contain a user-friendly Windows 10 environment. Microsoft Office tools (Excel, Word, PowerPoint) will be included in the AE. Licensing fees are included in the per seat subscription cost.

- Maintain HITRUST certified and HIPAA compliance. Internet access from inside the Enclave will be whitelisted based on GMCB permitted sites.

- Provide the following analytic tools in the AE:
  - The versions requested by the GMCB of: R, Python, SQL Workbench, and Anaconda.
  - Additional software can be installed in the AE at the request of the GMCB. Any applicable software license costs will be covered by the GMCB.
  - If software installation and configuration for the requested software is estimated to exceed eight hours or requires third party consultation, provide an estimated cost to accommodate the new software request.

- The database system provided in the AE will be Amazon Redshift, a columnar database service.

- The enclave will house two comprehensive VHCURES extract versions simultaneously, usually the current and prior quarter.

- Users will have a local storage drive in the AE. If permitted by the GMCB, users will have a shared drive mapped to an S3 bucket. Approved individuals may be allowed appropriate access to files placed on the shared drive.

- *Availability:* The AE will be generally available 24x7 with a guaranteed up-time of 99.9% during core business hours (defined as 8am – 5pm, Eastern Standard Time, Monday through Friday, excluding national holidays). Scheduled maintenance of the AE will generally be performed the third weekend of every month.

- *Maintenance and Back-up:* Scheduled maintenance will generally be performed the 3rd weekend of every month. Send maintenance reminders the week prior to maintenance occurring. Provide seven or more days' notice for any scheduled downtime. Data in the secure analytic environment will be backed-up daily.

- Store consolidated data in a format that is efficiently designed for querying and optimized for multiple parameter filtering.

- The State will identify and document any specific performance issues that are significant and persistent. Onpoint will work with the State to investigate and determine the root cause of such performance issues. To the extent that those causes are attributed, in whole or in part, to Onpoint, Onpoint will work to remediate those issues for which it is responsible. Create query performance benchmarks for user acceptance testing and performance monitoring, to be approved by the GMCB.

- Provide both utilization metrics as well as performance metrics for all components of the solution to the GMCB staff upon request. Utilization metrics will be both identifiable and summarized to address audit trail as well as trends in user activity.

- Maintain on and offsite backup copies of the files and datasets submitted by reporters and as consolidated and finalized by Onpoint in a secure location that meets security standards for Medicare data containing individual identifiers as specified in the CMS Data Use Agreement Form CMS-R-0235 under section #7 as the State's (CMS licensee) designated custodian (CMS custodian).

- Accommodate new data fields derived from existing data fields, as specified by the State. If the State develops an enterprise-wide master person index, in cases of disagreement, the default layouts and methods will be those of the data management vendor. Collaborate in developing specifications for the unique person identifier and for evaluating the accuracy of the identifier. Depending on the scope of the work, a cost proposal will be provided.

- Maintain a secure virtual, remote up-to-date patches, for the duration of contract.

- Participate in a State-appointed data users group and provide troubleshooting services for accessing or analyzing data.

- Ensure that historical datasets are archived and accessible to the analytic environment dating back to 2007. Historical data will be kept as long as technically feasible.

- Ensure that all planned maintenance services related to any components of the APCD solution, excluding routine monthly maintenance, must be reviewed and approved by GMCB prior to their execution. Work with the GMCB to schedule and notify users about such events.

- Maintain comprehensive change management processes.

- Maintain a comprehensive, formal process for user acceptance testing before and after production.

- Respond to all requests/questions in accordance with the Service Level Standards listed in Attachment F.

- Develop a transition contingency plan, including details on Vendor-specific resources, in the event the contract expires or is terminated.
    - Before conclusion of this contract and in the event that the contract is terminated or the contract is awarded to another vendor, Contractor shall develop a transition plan for continued operations that will assist the State in maintaining timely collection of the data during contract transition. As specified by the State, upon conclusion of the contract, the Contractor shall transfer a minimum of five years of raw data files as submitted by payers, relevant archives of communications with submitters, reference materials that document the data submission history at summary and individual submitters, and any VHCURES data specified by the State as permitted by State and federal agreements.
    - Ten months prior to contract expiration, or upon request by the State, whichever comes sooner, the Contractor must provide to the State a Transition Plan. The Transition Plan must include a detailed strategy and budget which addresses all of the following:

        a) A timetable for Transition.

        b) A detailed outline and specifications of all data to be turned over. Data must include a minimum of five years of raw submission files, as well as any data derived from the process of cleansing and loading contents of those files into Contractor's data warehouse. Consolidated data will be provided via regular extracts to the State, as described in Task 3.

        c) The Transition of data to the newly awarded VHCURES vendor.

        d) The provision of any updates to the current system's data before the newly awarded bidder begins operation.

        e) The identification of Contractor staff responsible for overseeing and executing this Transition Plan.

        f) A timetable for preparation of data transfer to the newly awarded bidder.

g) A plan for post-Transition support to resolve data conversion and production issues.
h) Training of the newly awarded bidder, if necessary and requested by the State, to extract information contained in the Transition Plan.
i) A timetable for acceptance testing with the newly awarded bidder to begin properly analyzing transactions.

- Upon receipt of the Transition Plan by the State, both parties agree to meet, discuss, and resolve any issues or concerns in order to meet the terms of this section. The parties agree to personally meet and negotiate in good faith regarding the provisions outlined within the Transition Plan.
- At the conclusion of the contract, Contractor shall, at the State's sole discretion, destroy all VHCURES data, including derived files generated from VHCURES in the possession or under the control of Contractor as acquired and processed under the contract.

- The Data Dictionary data documentation will include version control numbering information to allow for tracking of all changes made over time.

- Provide the State data documentation that includes comprehensive entity relationship diagrams covering, at a minimum, all extensions and linkages.

- Produce and maintain a Data Dictionary (similar to a Code Book Structure) documentation containing detailed specifications and documentation for the consolidated data sets, including description of files, tables, data elements, codes, and completeness of elements. In addition, any derived fields or flags will be explicitly defined, including the source fields. Specification regarding each field/flag must be outlined.

- Onpoint will work with the GMCB to develop the requirements for custom datasets/datamarts. Depending on the scope, a cost proposal will be developed.

- Onpoint is strictly prohibited from releasing or using data or information obtained in its capacity as a collector and processor of the data for any purposes other than those specifically authorized by the State, except Onpoint may disclose such data or information as required by law and may use such data or information for the proper management of Onpoint or to carry out its legal responsibilities as allowed by HIPAA. In no event will Onpoint sell the State's data or otherwise use it for purposes other than those authorized by this contract. Failure to comply could be a violation of Vermont laws and rules and lead to enforcement actions including potential voiding of the contract.

- Cooperate with other vendors as needed to determine data layouts and transmittal methods.

- Onpoint will be available upon the request of the State to consult with other parties working to build a master patient/person index or to identify unique individuals in eligibility and claims files who may have multiple payers or change payers over time to explain the method used to assign unique person identifiers in the VHCURES database.

- Create flags as needed for Health Service Areas in the State of Vermont, based on information provided by the Vermont Department of Health related to geographic assignments. The Department of Health may provide updated information on these service areas during any quarterly claims processing cycle.

- Implement claims grouping logic in the data warehouse to assist in the identification of health care events, products and services, demographic risk, clinical risk, and episodes of care.

- Apply and make available 3M's diagnosis related groups or other grouper designated by the State in the VHCURES data warehouse; shall implement provider attribution logic in VHCURES in accordance with schema provided by the Vermont Blueprint for Health as directed by the State. Use of proprietary groupers (e.g. 3M, ACGs) assumes any licensing costs are paid by state.

- Purchase and provide the State one (1) set of comprehensive coding manuals that include commercially available coding manuals for each year of release of the coding systems. Provide documentation for any proprietary software / data sets incorporated into the extract.

- Users will access the AE by means of an AWS Workspace Client connection with DUO multi-factor authentication. User must supply full name, email address, and cell phone number for the set-up of the multi-factor authentication process. Onpoint will add users to the AE within two business days after receipt of authentication information.

- Provide each user with the appropriate user-based or role-based permission to the latest two State comprehensive extracts as directed by the GMCB. State extracts will include Commercial, Medicaid and Medicare data. Configure access to the AE in accordance with the GMCB's user specific DUA. Non-state users will not have access to Medicare data within the enclave.

- Work with GMCB to configure additional tables or materialized views that permit the appropriate level of access to groups/users. The GMCB will be responsible for data management for all users in the AE, including approval of data requests and of data leaving the AE.

- GMCB will have functionality to download data analyses (reports, charts, graphs) from the AE and copy additional data to the AE. This functionality will be provided by leveraging an Amazon S3 bucket and a GMCB specific work schema in the Redshift database.

- Collaborate with GMCB staff to create and manage user roles and rights to the data.

- Employ access controls to allow a variety of user profiles with role-appropriate access to retain data security including full read-only access to the raw data tables (or views that mirror them) and the ability to create temporary tables.

- Support the GMCB's and other State agencies' full access to the extracted data within the operational data set including raw, as-submitted values as requested for all years. In particular, access will not be impeded by Onpoint due to proprietary coding or any other business-specific reason. Act in accordance with the understanding that the State of Vermont is the primary steward of the data. There will be some configurability of value adds and standard reporting based on the GMCB's preferences.

- Provide mechanism for approved users to import external data sources to support approved linkages to VHCURES data in the Analytic Enclave at little to no cost to the approved user or State.

- Provide access to the Client Data Management system to allow GMCB-approved staff to access up-to-date information regarding registration, submission, and data processing.

Task 4: Standard Reports for Green Mountain Care Board (monthly)

- Provide monthly status reports about data submission and conformance to specifications, to support GMCB oversight of non-compliant data submitters. These reports must also be provided as requested.

- Business intelligence tools used for business analytics shall be architected with the solution, not with the VHCURES database directly and available to remote users to provide report generation and data visualization. Provide ten standard reports, produced through Tableau and updated according to a frequency agreed upon with the State. The reports will be selected from the Contractor's library of existing reports, with any agreed upon adaptations.

- Provide training and technical support to the GMCB and GMCB-approved users. Services might include troubleshooting problems with the data submitters and users, users gaining access to the data, issues pertaining to modifications and the user's ability to analyze the data from the extract including accessing and authoring reports using Tableau.

Task 5: Ad Hoc Work for Green Mountain Care Board

- Ad hoc tasks are only to be initiated, performed, and completed upon the written execution per the Maintenance & Operations Plan. Examples of potential requests include the following:

- State chooses to integrate additional file types or data elements not currently being supplied by submitters.

- At the request of the State, Onpoint will collaborate on efforts to utilize non-claims-based provider information to supplement claims-based provider information for the purpose of improving provider identity management, and the master provider index.

- At the request of the State, Onpoint will coordinate with State initiatives related to master provider directory at the Agency of Human Services, the Vermont Health Information Exchange, the Vermont Health Benefit Exchange, and other purposes as directed by the State.

- At the request of the State, Onpoint will implement additional claims grouping logic, or incorporate other claims attribution schemas in the VHCURES data warehouse.

- Support ad hoc requests for customized data queries, reports, and analyses, and design and generate ad hoc reports during the contract period as requested by the State. Prior to initiating any work on ad hoc reporting, Onpoint will propose a methodology for performing the analysis, as well as a budget, and a timeline for completing the work. Onpoint will not begin working on any ad hoc reporting without written authorization from the State's contract manager. Ad hoc analyses may not exceed the dollar amount specified in Attachment B (Payment Provisions).

- Although Onpoint has the expertise to conduct highly sophisticated studies, Onpoint also understands that straightforward methods and timely delivery are often key to relevance, and shall always seek simple and efficient solutions where available. In order to streamline the production of ad hoc studies without compromising other work, for each ad hoc task, Onpoint will designate a task leader who will work closely with the project manager and other key staff to fulfill ad hoc requests. The task leader shall be responsible for defining the goals and methods

for each ad hoc report, discussing plans with the State and ensuring that Onpoint is authorized to proceed, completing studies, and preparing appropriate reports.

Task 6: Transition from Hashed to Live Identifiers

- When GMCB is prepared to move forward, Onpoint to develop new data mappings for all file and paper types (i.e. commercial, Medicaid, and Medicare).
- Update quality assurance processes across all stages (e.g., completeness and validity, data quality validation, trending, etc.).
- Develop a cross-walk between historical hashed and live identifiers.
- Update member clustering methodologies.
- Deliverables to be specified and agreed using the Delivery Expectation Document and Delivery Acceptance Form (DAF) model.

Task 7: Rule Change and Redesign of Data Layout

- When GMCB is prepared to move forward, Onpoint to completely revise the VHCURES layouts.
- Deliverables to be specified and agreed using the Delivery Expectation Document and Delivery Acceptance Form (DAF) model.
- Assumes any new data elements requested by the GMCB already exist in Onpoint's data model.
- Does not include pricing for revisions to Onpoint's hashing application. Assumes that redesign of layout includes live identifiers.
- Assumes redesign of current files being collected (e.g. Eligibility, Medical, Pharmacy).

Task 8: Addition of Dental Eligibility and Claims Submissions

- When GMCB is prepared to move forward, Onpoint to add dental data to VHCURES.
- Update data submission guide and hashing application.
- Dental claim layout will be Onpoint's standard layout or the APCD Common Data Layout (CDL)
- Registration, training and onboarding of up to 10 new dental-data submitters.
- Ongoing submitter support and quality assurance of data submissions
- Inclusion of dental data in the quarterly VHCURES extracts with related documentation.

Deliverables to be specified and agreed using the Delivery Expectation Document and Delivery Acceptance Form (DAF) model.

Task 9: Transition Tasks: Medicare Claim Submission and Extract Updates to Support the Vermont All-Payer ACO Model

New data elements will be incorporated into VT Medicare Submission, and they will be delivered in a new table in the VHCURES extract.

Assumptions

- There will be no changes to the data model to accommodate the new data elements.
- No changes will be made to the hashing application.
- Dollar amounts will not be mapped to the "prepaid" field.
- End users of the data will calculate reduction amounts using the new ACO table.

Scope of Work

- Map the new Medicare fields to the Onpoint submission file.
- Update the submission generator to translate CCW Medicare format into Onpoint VT Medicare submission format.
- Update the extract process to output to a stand-alone vertical table.
- Provide data dictionary for extracted table.
- Document the process for calculating reduction amounts using the new ACO table and review with end users.

Task 10: Vulnerability Testing

Onpoint shall run (or prove evidence of having been run) quarterly vulnerability assessments on externally facing assets storing or presenting state data including hosted or on premises infrastructure. Results will be delivered quarterly to the ADS security team, or technical lead for the program. Contractor shall remediate all critical/high issues within 90 days. Contractor shall provide a risk mitigation plan for medium and low issues. Contractor shall obtain written State approval for any exceptions. Contractor will work with the state to define a reporting process.

Onpoint will provide a copy of its HITRUST certification letter, HITRUST executive summary report, and annual penetration testing, annually, upon request.

EXHIBIT 4
Third Party Software Licensed by the State of Vermont

A list of all Third Party Software currently or potentially licensed by the State for purposes of Contractor's performance of the Services is cited below. Contractor will assume operational responsibility for such Third Party Software and any related maintenance obligations to the same extent as if Contractor were the licensee of such Third Party Software as long as there is a signed software access and confidentiality agreement between the Green Mountain Care Board (GMCB) and Onpoint Health Data. In cases where software is paid for by Onpoint, then Onpoint will also assume financial responsibility for such Third Party Software. Contractor will cease use of such Third Party Software upon expiration or termination of this Contract.

- Tableau
  - Tableau Creator
  - Tableau Explorer
  - Tableau Viewer

- Risk Grouping Software selected by the GMCB
  - 3M Grouper
    - Clinical Risk Groups (CRGs)
    - All Patients Refined Diagnosis Related Groups (APR DRGs)

    OR

  - Johns Hopkins ACG® System

ATTACHMENT B
PAYMENT PROVISIONS

The maximum dollar amount payable under this contract is not intended as any form of a guaranteed amount. The Contractor will be paid for products or services actually delivered or performed, as specified in Attachment A, up to the maximum allowable amount specified on page 1 of this contract. The payment schedule for services performed, and any additional reimbursements, are included in this Attachment. The following provisions specifying payment are:

1. Prior to commencement of work and release of any payments, Contractor shall submit to the State:

a. a certificate of insurance consistent with the requirements set forth in Attachment C, Section 8 (Insurance), and with any additional requirements for insurance as may be set forth elsewhere in this contract; and

b. a current IRS Form W-9 (signed within the last six months).

2. Payment terms are **Net 30** days from the date the State receives an error-free invoice with all necessary and complete supporting documentation. Payments for subcontractors, if any, will only be made upon approval (See Attachment C, #15).

3. The Contractor will be paid based on documentation and itemization of work performed and included in invoicing as required by 32 VSA §463. On a monthly basis, the Contractor shall submit a detailed invoice itemizing all work performed during the invoice period, including the dates of service and, where applicable, rates of pay, hours of work performed, and any other information and/or documentation appropriate and sufficient to substantiate the amount invoiced for payment by the State. All invoices must include the Contract # for this contract.

The maximum amount payable under the Ad Hoc tasks of this contract shall not exceed $356,250.00 over five years. The State does not guarantee the assignment of any minimum number of hours or other work under this contract.

4. Invoices shall be submitted to the State at the following email address: gmcb.invoice@vermont.gov

5. Contractor shall submit invoices to the State upon State Acceptance of a deliverable in accordance with the schedule for delivered products, or rates for services performed set forth below:

Table 1: Payment Schedule, Summary							
	Implementa-tion Services	**Fixed Cost, Monthly Fees**	**Payment Timing Based on GMCB Acceptance of Deliverable**	**Total Available for Ad Hoc Tasks**	**Total Available for Optional Tasks - Implementation**	**Total Available for Optional Tasks – Annual Dental Fees**	**Total**
	(Table 2)	**(Table 3)**	**(Table 4)**	**(Table 5)**	**(Table 6)**	**(Table 6)**	
Year 1	$61,400	$728,804	$49,010				
Year 2		732,500	49,010				
Year 3		736,208	49,010				
Year 4		739,892	49,010				
Year 5		743,596	49,010				
Total	$61,400	$3,681,000	$245,050	$356,250	$190,100	$86,000	$4,619,800

Table 2: Payment Schedule, Implementation – Payable Upon GMCB Acceptance of Phase		
Task	**Deliverable Date**	**Payment**
Transition Tasks Deliverable (Exhibit 2) Update VT Medicare Data Submission to include All-Payer ACO claim fields		$11,200
Implementation (Exhibit 2)		
Project Initiation		5,020
New Analytic Tools Implementation		5,020
Transition and Train Users to New Claims Data Manager (CDM)		10,040
Initial Analytic Enclave (AE) and Tableau Setup		10,040
BI Standard Reports, first five (5) reports		5,020
BI Standard Reports, second five (5) reports		5,020
Post Implementation Support		5,020
Project Close Out (Payment for 10% retainage for implementation is made)		5,020
Total		**$50,200**
Total		**$61,400**

Table 3: Payment Schedule, Monthly Costs – invoiced the first of every month for prior month services					
License and Hosting Fees	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
Monthly Totals					
Fixed:					
Enterprise Application: License Fees	$16,667	$16,667	$16,667	$16,667	$16,667
Data Aggregation Services	27,867	28,175	28,484	28,791	29,100
Data Analytics Services	3,025	3,025	3,025	3,025	3,025
Variable:					
Business Intelligence (BI) Tool (Tableau)	1,175	1,175	1,175	1,175	1,175
Hosting Fees-Amazon Web Services (AWS) Analytic Enclave seats (Q=26-30)	12,000	12,000	12,000	12,000	12,000
Total License and Hosting Fees	**$60,734**	**$61,042**	**$61,351**	**$61,658**	**$61,966**
Annual Total	**$728,804**	**$732,500**	**$736,208**	**$739,892**	**$743,596**
Retainage of 10% will be withheld from every monthly payment, then paid with payment for subsequent quarterly extract					

Table 4: Payment Schedule, Timing Based on GMCB Acceptance of Deliverable Tasks		
Task	**Invoicing Frequency**	**Annual Total Amount**
Annual Registration Process (25% December, 25% January, 50% upon Acceptance of Annual Registration Report using DED and DAF)	See Left	$11,200
Consolidated Claims Data Set (Extract) including Data Dictionary and other items that support the data. Payable upon GMCB acceptance of Extract and Task 10 Vulnerability Testing (DED, DAF)	Quarterly	$21,000
Standard Reports Issued for Green Mountain Care Board (including monthly status reports, as detailed in the Project Plan)	Quarterly (tied to the extract)	$16,810
Total		**$49,010**

Table 5: Ad Hoc

Total available over contract term is $356,250 at billable rates listed below.

Title	Project Role	Example Name	Billable Rate
Client Account Manager	Dedicated Project Manager	Carolyne Conrad	$175
Senior Director of Client Services	Lead Client Support	Janice Bourgault, CPC	$250
Director of Data Analytics & Operations	Operations Management & Quality Assurance Lead	Joanna Duncan, PhD, CPC	$250

Title	Project Role	Example Name	Billable Rate
Chief Information Officer	Technical Infrastructure Lead & Data Security Officer	Jeff Stoddard, HCISPP	$250
Director of Analytic Development	Analytic Solution Lead	Karl Finison, MA	$250
Lead Systems Developer	System Development Lead	Jeff Cain	$175
Senior Health Data Analyst	Data Analyst Lead	Katherine Lydon, MPH	$175
Operations Analyst	Dedicated Operations Analyst	Dawn Hamlin	$125
Health Data Analyst	Dedicated Data Analyst	Adam Bakopolus	$150

Table 6: Payment Schedule for Conditional Tasks

Task	Invoicing Frequency	Implementation Not to Exceed	Annual Not to Exceed
Task 6: Transition from Hashed to Live Identifiers – Initial Implementation	Per DED, DAF	$62,500	$0
Task 7: Rule Change and Redesign of Data Layout	Per DED, DAF	$80,000	$0
Task 8: Addition of Dental Eligibility and Claims Submissions. Implementation includes $4,300 for one quarter cost. Annual ongoing cost = $4,300 per quarter	Per DED, DAF	$47,600	$17,200
Total		**$190,100**	**$17,200**

EXPENSES: The fee for services shall be inclusive of Contractor expenses.

RETAINAGE: In the discretion of the State, a contract resulting from this RFP may provide that the State withhold a percentage of the total amount payable for some or all deliverables, such retainage to be payable upon satisfactory completion and State acceptance in accordance with the terms and conditions of the contract. Contractor agrees to a 10% retainage of the total cost of those services specified in Tables two (2) and three (3) above as being subject to retainage pending State's review, approval, and acceptance of Contractor's quarterly extract. The State shall determine retainage, including any withholding or proration, of the total cost of these services by determining whether Contractor's performance has met, to State's satisfaction, Contractor's requirements under Attachment A. Upon satisfactory completion of all services subject to retainage, Contractor shall submit a retainage statement to request funds withheld.

ATTACHMENT C:
STANDARD STATE PROVISIONS
FOR CONTRACTS AND GRANTS
REVISED DECEMBER 15, 2017

1. Definitions: For purposes of this Attachment, "Party" shall mean the Contractor, Grantee or Subrecipient, with whom the State of Vermont is executing this Agreement and consistent with the form of the Agreement. "Agreement" shall mean the specific contract or grant to which this form is attached.

2. Entire Agreement: This Agreement, whether in the form of a contract, State-funded grant, or Federally-funded grant, represents the entire agreement between the parties on the subject matter. All prior agreements, representations, statements, negotiations, and understandings shall have no effect.

3. Governing Law, Jurisdiction and Venue; No Waiver of Jury Trial: This Agreement will be governed by the laws of the State of Vermont. Any action or proceeding brought by either the State or the Party in connection with this Agreement shall be brought and enforced in the Superior Court of the State of Vermont, Civil Division, Washington Unit. The Party irrevocably submits to the jurisdiction of this court for any action or proceeding regarding this Agreement. The Party agrees that it must first exhaust any applicable administrative remedies with respect to any cause of action that it may have against the State with regard to its performance under this Agreement. Party agrees that the State shall not be required to submit to binding arbitration or waive its right to a jury trial.

4. Sovereign Immunity: The State reserves all immunities, defenses, rights or actions arising out of the State's sovereign status or under the Eleventh Amendment to the United States Constitution. No waiver of the State's immunities, defenses, rights or actions shall be implied or otherwise deemed to exist by reason of the State's entry into this Agreement.

5. No Employee Benefits For Party: The Party understands that the State will not provide any individual retirement benefits, group life insurance, group health and dental insurance, vacation or sick leave, workers compensation or other benefits or services available to State employees, nor will the State withhold any state or Federal taxes except as required under applicable tax laws, which shall be determined in advance of execution of the Agreement. The Party understands that all tax returns required by the Internal Revenue Code and the State of Vermont, including but not limited to income, withholding, sales and use, and rooms and meals, must be filed by the Party, and information as to Agreement income will be provided by the State of Vermont to the Internal Revenue Service and the Vermont Department of Taxes.

6. Independence: The Party will act in an independent capacity and not as officers or employees of the State.

7. Defense and Indemnity: The Party shall defend the State and its officers and employees against all third party claims or suits arising in whole or in part from any act or omission of the Party or of any agent of the Party in connection with the performance of this Agreement. The State shall notify the Party in the event of any such claim or suit, and the Party shall immediately retain counsel and otherwise provide a complete defense against the entire claim or suit. The State retains the right to participate at its own expense in the defense of any claim. The State shall have the right to approve all proposed settlements of such claims or suits.

After a final judgment or settlement, the Party may request recoupment of specific defense costs and may file suit in Washington Superior Court requesting recoupment. The Party shall be entitled to recoup costs

only upon a showing that such costs were entirely unrelated to the defense of any claim arising from an act or omission of the Party in connection with the performance of this Agreement.

The Party shall indemnify the State and its officers and employees if the State, its officers or employees become legally obligated to pay any damages or losses arising from any act or omission of the Party or an agent of the Party in connection with the performance of this Agreement.

Notwithstanding any contrary language anywhere, in no event shall the terms of this Agreement or any document furnished by the Party in connection with its performance under this Agreement obligate the State to (1) defend or indemnify the Party or any third party, or (2) otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or other costs of the Party or any third party.

8. Insurance: Before commencing work on this Agreement the Party must provide certificates of insurance to show that the following minimum coverages are in effect. It is the responsibility of the Party to maintain current certificates of insurance on file with the State through the term of this Agreement. No warranty is made that the coverages and limits listed herein are adequate to cover and protect the interests of the Party for the Party's operations. These are solely minimums that have been established to protect the interests of the State.

Workers Compensation: With respect to all operations performed, the Party shall carry workers' compensation insurance in accordance with the laws of the State of Vermont. Vermont will accept an out-of-state employer's workers' compensation coverage while operating in Vermont provided that the insurance carrier is licensed to write insurance in Vermont and an amendatory endorsement is added to the policy adding Vermont for coverage purposes. Otherwise, the party shall secure a Vermont workers' compensation policy, if necessary to comply with Vermont law.

General Liability and Property Damage: With respect to all operations performed under this Agreement, the Party shall carry general liability insurance having all major divisions of coverage including, but not limited to:

Premises - Operations

Products and Completed Operations

Personal Injury Liability

Contractual Liability

The policy shall be on an occurrence form and limits shall not be less than:

$1,000,000 Each Occurrence

$2,000,000 General Aggregate

$1,000,000 Products/Completed Operations Aggregate

$1,000,000 Personal & Advertising Injury

Automotive Liability: The Party shall carry automotive liability insurance covering all motor vehicles, including hired and non-owned coverage, used in connection with the Agreement. Limits of coverage shall not be less than $500,000 combined single limit. If performance of this Agreement involves construction, or the transport of persons or hazardous materials, limits of coverage shall not be less than $1,000,000 combined single limit.

Additional Insured. The General Liability and Property Damage coverages required for performance of this Agreement shall include the State of Vermont and its agencies, departments, officers and employees as Additional Insureds. If performance of this Agreement involves construction, or the transport of

persons or hazardous materials, then the required Automotive Liability coverage shall include the State of Vermont and its agencies, departments, officers and employees as Additional Insureds. Coverage shall be primary and non-contributory with any other insurance and self-insurance.

Notice of Cancellation or Change. There shall be no cancellation, change, potential exhaustion of aggregate limits or non-renewal of insurance coverage(s) without thirty (30) days written prior written notice to the State.

9. Reliance by the State on Representations: All payments by the State under this Agreement will be made in reliance upon the accuracy of all representations made by the Party in accordance with this Agreement, including but not limited to bills, invoices, progress reports and other proofs of work.

10. False Claims Act: The Party acknowledges that it is subject to the Vermont False Claims Act as set forth in 32 V.S.A. § 630 *et seq.* If the Party violates the Vermont False Claims Act it shall be liable to the State for civil penalties, treble damages and the costs of the investigation and prosecution of such violation, including attorney's fees, except as the same may be reduced by a court of competent jurisdiction. The Party's liability to the State under the False Claims Act shall not be limited notwithstanding any agreement of the State to otherwise limit Party's liability.

11. Whistleblower Protections: The Party shall not discriminate or retaliate against one of its employees or agents for disclosing information concerning a violation of law, fraud, waste, abuse of authority or acts threatening health or safety, including but not limited to allegations concerning the False Claims Act. Further, the Party shall not require such employees or agents to forego monetary awards as a result of such disclosures, nor should they be required to report misconduct to the Party or its agents prior to reporting to any governmental entity and/or the public.

12. Location of State Data: No State data received, obtained, or generated by the Party in connection with performance under this Agreement shall be processed, transmitted, stored, or transferred by any means outside the continental United States, except with the express written permission of the State.

13. Records Available for Audit: The Party shall maintain all records pertaining to performance under this agreement. "Records" means any written or recorded information, regardless of physical form or characteristics, which is produced or acquired by the Party in the performance of this agreement. Records produced or acquired in a machine readable electronic format shall be maintained in that format. The records described shall be made available at reasonable times during the period of the Agreement and for three years thereafter or for any period required by law for inspection by any authorized representatives of the State or Federal Government. If any litigation, claim, or audit is started before the expiration of the three-year period, the records shall be retained until all litigation, claims or audit findings involving the records have been resolved.

14. Fair Employment Practices and Americans with Disabilities Act: Party agrees to comply with the requirement of 21 V.S.A. Chapter 5, Subchapter 6, relating to fair employment practices, to the full extent applicable. Party shall also ensure, to the full extent required by the Americans with Disabilities Act of 1990, as amended, that qualified individuals with disabilities receive equitable access to the services, programs, and activities provided by the Party under this Agreement.

15. Set Off: The State may set off any sums which the Party owes the State against any sums due the Party under this Agreement; provided, however, that any set off of amounts due the State of Vermont as taxes shall be in accordance with the procedures more specifically provided hereinafter.

16. Taxes Due to the State:

- **A.** Party understands and acknowledges responsibility, if applicable, for compliance with State tax laws, including income tax withholding for employees performing services within the State, payment of use tax on property used within the State, corporate and/or personal income tax on income earned within the State.
- **B.** Party certifies under the pains and penalties of perjury that, as of the date this Agreement is signed, the Party is in good standing with respect to, or in full compliance with, a plan to pay any and all taxes due the State of Vermont.
- **C.** Party understands that final payment under this Agreement may be withheld if the Commissioner of Taxes determines that the Party is not in good standing with respect to or in full compliance with a plan to pay any and all taxes due to the State of Vermont.
- **D.** Party also understands the State may set off taxes (and related penalties, interest and fees) due to the State of Vermont, but only if the Party has failed to make an appeal within the time allowed by law, or an appeal has been taken and finally determined and the Party has no further legal recourse to contest the amounts due.

17. Taxation of Purchases: All State purchases must be invoiced tax free. An exemption certificate will be furnished upon request with respect to otherwise taxable items.

18. Child Support: (Only applicable if the Party is a natural person, not a corporation or partnership.) Party states that, as of the date this Agreement is signed, he/she:

- **A.** is not under any obligation to pay child support; or
- **B.** is under such an obligation and is in good standing with respect to that obligation; or
- **C.** has agreed to a payment plan with the Vermont Office of Child Support Services and is in full compliance with that plan.

Party makes this statement with regard to support owed to any and all children residing in Vermont. In addition, if the Party is a resident of Vermont, Party makes this statement with regard to support owed to any and all children residing in any other state or territory of the United States.

19. Sub-Agreements: Party shall not assign, subcontract or subgrant the performance of this Agreement or any portion thereof to any other Party without the prior written approval of the State. Party shall be responsible and liable to the State for all acts or omissions of subcontractors and any other person performing work under this Agreement pursuant to an agreement with Party or any subcontractor.
In the case this Agreement is a contract with a total cost in excess of $250,000, the Party shall provide to the State a list of all proposed subcontractors and subcontractors' subcontractors, together with the identity of those subcontractors' workers compensation insurance providers, and additional required or requested information, as applicable, in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54).
Party shall include the following provisions of this Attachment C in all subcontracts for work performed solely for the State of Vermont and subcontracts for work performed in the State of Vermont: Section 10 ("False Claims Act"); Section 11 ("Whistleblower Protections"); Section 12 ("Location of State Data"); Section 14 ("Fair Employment Practices and Americans with Disabilities Act"); Section 16 ("Taxes Due the State"); Section 18 ("Child Support"); Section 20 ("No Gifts or Gratuities"); Section 22 ("Certification Regarding Debarment"); Section 30 ("State Facilities"); and Section 32.A ("Certification Regarding Use of State Funds").

20. No Gifts or Gratuities: Party shall not give title or possession of anything of substantial value (including property, currency, travel and/or education programs) to any officer or employee of the State during the term of this Agreement.

21. Copies: Party shall use reasonable best efforts to ensure that all written reports prepared under this Agreement are printed using both sides of the paper.

22. Certification Regarding Debarment: Party certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, neither Party nor Party's principals (officers, directors, owners, or partners) are presently debarred, suspended, proposed for debarment, declared ineligible or excluded from participation in Federal programs, or programs supported in whole or in part by Federal funds.
Party further certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, Party is not presently debarred, suspended, nor named on the State's debarment list at: http://bgs.vermont.gov/purchasing/debarment

23. Conflict of Interest: Party shall fully disclose, in writing, any conflicts of interest or potential conflicts of interest.

24. Confidentiality: Party acknowledges and agrees that this Agreement and any and all information obtained by the State from the Party in connection with this Agreement are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq.

25. Force Majeure: Neither the State nor the Party shall be liable to the other for any failure or delay of performance of any obligations under this Agreement to the extent such failure or delay shall have been wholly or principally caused by acts or events beyond its reasonable control rendering performance illegal or impossible (excluding strikes or lock-outs) ("Force Majeure"). Where Force Majeure is asserted, the nonperforming party must prove that it made all reasonable efforts to remove, eliminate or minimize such cause of delay or damages, diligently pursued performance of its obligations under this Agreement, substantially fulfilled all non-excused obligations, and timely notified the other party of the likelihood or actual occurrence of an event described in this paragraph.

26. Marketing: Party shall not refer to the State in any publicity materials, information pamphlets, press releases, research reports, advertising, sales promotions, trade shows, or marketing materials or similar communications to third parties except with the prior written consent of the State.

27. Termination:

A. **Non-Appropriation:** If this Agreement extends into more than one fiscal year of the State (July 1 to June 30), and if appropriations are insufficient to support this Agreement, the State may cancel at the end of the fiscal year, or otherwise upon the expiration of existing appropriation authority. In the case that this Agreement is a Grant that is funded in whole or in part by Federal funds, and in the event Federal funds become unavailable or reduced, the State may suspend or cancel this Grant immediately, and the State shall have no obligation to pay Subrecipient from State revenues.
B. **Termination for Cause:** Either party may terminate this Agreement if a party materially breaches its obligations under this Agreement, and such breach is not cured within thirty (30) days after delivery of the non-breaching party's notice or such longer time as the non-breaching party may specify in the notice.
C. **Termination Assistance:** Upon nearing the end of the final term or termination of this Agreement, without respect to cause, the Party shall take all reasonable and prudent measures to facilitate any transition required by the State. All State property, tangible and intangible, shall be returned to the State upon demand at no additional cost to the State in a format acceptable to the State.

28. Continuity of Performance: In the event of a dispute between the Party and the State, each party will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.

29. No Implied Waiver of Remedies: Either party's delay or failure to exercise any right, power or remedy under this Agreement shall not impair any such right, power or remedy, or be construed as a waiver of any such right, power or remedy. All waivers must be in writing.

30. State Facilities: If the State makes space available to the Party in any State facility during the term of this Agreement for purposes of the Party's performance under this Agreement, the Party shall only use the space in accordance with all policies and procedures governing access to and use of State facilities which shall be made available upon request. State facilities will be made available to Party on an "AS IS, WHERE IS" basis, with no warranties whatsoever.

31. Requirements Pertaining Only to Federal Grants and Subrecipient Agreements: If this Agreement is a grant that is funded in whole or in part by Federal funds:

A. Requirement to Have a Single Audit: The Subrecipient will complete the Subrecipient Annual Report annually within 45 days after its fiscal year end, informing the State of Vermont whether or not a Single Audit is required for the prior fiscal year. If a Single Audit is required, the Subrecipient will submit a copy of the audit report to the granting Party within 9 months. If a single audit is not required, only the Subrecipient Annual Report is required.
For fiscal years ending before December 25, 2015, a Single Audit is required if the subrecipient expends $500,000 or more in Federal assistance during its fiscal year and must be conducted in accordance with OMB Circular A-133. For fiscal years ending on or after December 25, 2015, a Single Audit is required if the subrecipient expends $750,000 or more in Federal assistance during its fiscal year and must be conducted in accordance with 2 CFR Chapter I, Chapter II, Part 200, Subpart F. The Subrecipient Annual Report is required to be submitted within 45 days, whether or not a Single Audit is required.

B. Internal Controls: In accordance with 2 CFR Part II, §200.303, the Party must establish and maintain effective internal control over the Federal award to provide reasonable assurance that the Party is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the award. These internal controls should be in compliance with guidance in "Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States and the "Internal Control Integrated Framework", issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

C. Mandatory Disclosures: In accordance with 2 CFR Part II, §200.113, Party must disclose, in a timely manner, in writing to the State, all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. Failure to make required disclosures may result in the imposition of sanctions which may include disallowance of costs incurred, withholding of payments, termination of the Agreement, suspension/debarment, etc.

32. Requirements Pertaining Only to State-Funded Grants:

A. Certification Regarding Use of State Funds: If Party is an employer and this Agreement is a State-funded grant in excess of $1,001, Party certifies that none of these State funds will be used to interfere with or restrain the exercise of Party's employee's rights with respect to unionization.

B. Good Standing Certification (Act 154 of 2016): If this Agreement is a State-funded grant, Party hereby represents: (i) that it has signed and provided to the State the form prescribed by the Secretary of Administration for purposes of certifying that it is in good standing (as provided in Section 13(a)(2) of Act 154) with the Agency of Natural Resources and the Agency of Agriculture, Food and Markets, or otherwise explaining the circumstances surrounding the inability to so certify, and (ii) that it will comply with the requirements stated therein.

(End of Standard Provisions)

ATTACHMENT D
INFORMATION TECHNOLOGY SYSTEM IMPLEMENTATION
TERMS AND CONDITIONS (rev. 3/08/19)

1. MODIFICATIONS TO CONTRACTOR DOCUMENTS

The parties specifically agree that the Contractor Documents are hereby modified and superseded by Attachment C and this Attachment D.

"Contractor Documents" shall mean one or more document, agreement or other instrument required by Contractor in connection with the performance of the products and services being purchased by the State, regardless of format, including the license agreement, end user license agreement or similar document, any hyperlinks to documents contained in the Contractor Documents, agreement or other instrument and any other paper or "shrinkwrap," "clickwrap," "browsewrap" or other electronic version thereof.

2. NO SUBSEQUENT, UNILATERAL MODIFICATION OF TERMS BY CONTRACTOR

Notwithstanding any other provision or other unilateral license terms which may be issued by Contractor during the Term of this Contract, and irrespective of whether any such provisions have been proposed prior to or after the issuance of an order for the products and services being purchased by the State, as applicable, the components of which are licensed under the Contractor Documents, or the fact that such other agreement may be affixed to or accompany the products and services being purchased by the State, as applicable, upon delivery, the terms and conditions set forth herein shall supersede and govern licensing and delivery of all products and services hereunder.

3. TERM OF CONTRACTOR'S DOCUMENTS; PAYMENT TERMS

Contractor acknowledges and agrees that, to the extent a Contractor Document provides for alternate term or termination provisions, including automatic renewals, such sections shall be waived and shall have no force and effect. All Contractor Documents shall run concurrently with the term of this Contract; provided, however, to the extent the State has purchased a perpetual license to use the Contractor's software, hardware or other services, such license shall remain in place unless expressly terminated in accordance with the terms of this Contract. Contractor acknowledges and agrees that, to the extent a Contractor Document provides for payment terms which differ from the payment terms set forth in Attachment B, such sections shall be waived and shall have no force and effect and the terms in Attachment B shall govern.

4. OWNERSHIP AND LICENSE IN DELIVERABLES

4.1 CONTRACTOR INTELLECTUAL PROPERTY

As between the parties, and subject to the terms and conditions of this Contract, Contractor and its third-party suppliers will retain ownership of all intellectual property rights in the [System], and any and all derivative works made to the [System] or any part thereof, as well as all Work Product provided to the State ("**Contractor Proprietary Technology**"). The State acquires no rights to Contractor Proprietary Technology except for the licensed interests granted under this Contract. The term "**Work Product**" means all other materials, reports, manuals, visual aids, documentation, ideas, concepts, techniques, inventions, processes, or works of authorship developed, provided or created by Contractor or its employees or contractors during the course of performing work for the State (excluding any State Data or derivative works thereof and excluding any output from the [System] generated by the State's use of the [System], including without limitation, reports, graphs, charts and modified State Data, but expressly

including any form templates of such reports, graphs or charts by themselves that do not include the State Data).

Title, ownership rights, and all Intellectual Property Rights in and to the [System] will remain the sole property of Contractor or its suppliers. The State acknowledges that the source code is not covered by any license hereunder and will not be provided by Contractor. Except as set forth in this Contract, no right or implied license or right of any kind is granted to the State regarding the [System] or any part thereof. Nothing in this Contract confers upon either party any right to use the other party's trade names and trademarks, except for permitted license use in accordance with this Contract. All use of such marks by either party will inure to the benefit of the owner of such marks, use of which will be subject to specifications controlled by the owner.

4.2 STATE INTELLECTUAL PROPERTY

The State shall retain all right, title and interest in and to (i) all content and all property, data and information furnished by or on behalf of the State or any agency, commission or board thereof, and to all information that is created under this Contract, including, but not limited to, all data that is generated under this Contract as a result of the use by Contractor, the State or any third party of any technology systems or knowledge bases that are developed for the State and used by Contractor hereunder, and all other rights, tangible or intangible; and (ii) all State trademarks, trade names, logos and other State identifiers, Internet uniform resource locators, State user name or names, Internet addresses and e-mail addresses obtained or developed pursuant to this Contract (collectively, "**State Intellectual Property**").

Contractor may not collect, access or use State Intellectual Property for any purpose other than as specified in this Contract. Upon expiration or termination of this Contract, Contractor shall return or destroy all State Intellectual Property and all copies thereof, and Contractor shall have no further right or license to such State Intellectual Property.

Contractor acquires no rights or licenses, including, without limitation, intellectual property rights or licenses, to use State Intellectual Property for its own purposes. In no event shall the Contractor claim any security interest in State Intellectual Property.

5. CONFIDENTIALITY AND NON-DISCLOSURE; SECURITY BREACH REPORTING

5.1 For purposes of this Contract, confidential information will not include information or material which (a) enters the public domain (other than as a result of a breach of this Contract); (b) was in the receiving party's possession prior to its receipt from the disclosing party; (c) is independently developed by the receiving party without the use of confidential information; (d) is obtained by the receiving party from a third party under no obligation of confidentiality to the disclosing party; or (e) is not exempt from disclosure under applicable State law.

5.2 CONFIDENTIALITY OF CONTRACTOR INFORMATION

The Contractor acknowledges and agrees that this Contract and any and all Contractor information obtained by the State in connection with this Contract are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq. The State will not disclose information for which a reasonable claim of exemption can be made pursuant to 1 V.S.A. § 317(c), including, but not limited to, trade secrets, proprietary information or financial information, including any formulae, plan, pattern, process, tool, mechanism, compound, procedure, production data, or compilation of information which is not patented, which is known only to the Contractor, and which gives the Contractor an opportunity to obtain business advantage over competitors who do not know it or use it.

The State shall immediately notify Contractor of any request made under the Access to Public Records Act, or any request or demand by any court, governmental agency or other person asserting a demand or request for Contractor information. Contractor may, in its discretion, seek an appropriate protective order, or otherwise defend any right it may have to maintain the confidentiality of such information under applicable State law within three business days of the State's receipt of any such request. Contractor agrees that it will not make any claim against the State if the State makes available to the public any information in accordance with the Access to Public Records Act or in response to a binding order from a court or governmental body or agency compelling its production. Contractor shall indemnify the State for any costs or expenses incurred by the State, including, but not limited to, attorneys' fees awarded in accordance with 1 V.S.A. § 320, in connection with any action brought in connection with Contractor's attempts to prevent or unreasonably delay public disclosure of Contractor's information if a final decision of a court of competent jurisdiction determines that the State improperly withheld such information and that the improper withholding was based on Contractor's attempts to prevent public disclosure of Contractor's information.

The State agrees that (a) it will use the Contractor information only as may be necessary in the course of performing duties, receiving services or exercising rights under this Contract; (b) it will provide at a minimum the same care to avoid disclosure or unauthorized use of Contractor information as it provides to protect its own similar confidential and proprietary information; (c) except as required by the Access to Records Act, it will not disclose such information orally or in writing to any third party unless that third party is subject to a written confidentiality agreement that contains restrictions and safeguards at least as restrictive as those contained in this Contract; (d) it will take all reasonable precautions to protect the Contractor's information; and (e) it will not otherwise appropriate such information to its own use or to the use of any other person or entity.

Contractor may affix an appropriate legend to Contractor information that is provided under this Contract to reflect the Contractor's determination that any such information is a trade secret, proprietary information or financial information at time of delivery or disclosure.

5.3 CONFIDENTIALITY OF STATE INFORMATION

In performance of this Contract, and any exhibit or schedule hereunder, the Contractor acknowledges that certain State Data (as defined below), to which the Contractor may have access may contain individual federal tax information, personal protected health information and other individually identifiable information protected by State or federal law or otherwise exempt from disclosure under the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq. ("State Data"). State Data shall not be stored, accessed from, or transferred to any location outside the United States.

Unless otherwise instructed by the State, Contractor agrees to keep confidential all State Data. The Contractor agrees that (a) it will use the State Data only as may be necessary in the course of performing duties or exercising rights under this Contract; (b) it will provide at a minimum the same care to avoid disclosure or unauthorized use of State Data as it provides to protect its own similar confidential and proprietary information; (c) it will not publish, reproduce, or otherwise divulge any State Data in whole or in part, in any manner or form orally or in writing to any third party unless it has received written approval from the State and that third party is subject to a written confidentiality agreement that contains restrictions and safeguards at least as restrictive as those contained in this Contract; (d) it will take all reasonable precautions to protect the State's information; and (e) it will not otherwise appropriate such information to its own use or to the use of any other person or entity. Contractor will take reasonable measures as are necessary to restrict access to State Data in the Contractor's possession to only those employees on its staff

who must have the information on a "need to know" basis. The Contractor shall not retain any State Data except to the extent required to perform the services under this Contract.

Contractor shall not access State user accounts or State Data, except in the course of data center operations, response to service or technical issues, as required by the express terms of this Contract, or at State's written request.

Contractor may not share State Data with its parent company or other affiliate without State's express written consent.

The Contractor shall promptly notify the State of any request or demand by any court, governmental agency or other person asserting a demand or request for State Data to which the Contractor or any third party hosting service of the Contractor may have access, so that the State may seek an appropriate protective order.

6. SECURITY OF STATE INFORMATION

6.1 SECURITY STANDARDS

To the extent the Contractor or its subcontractors, affiliates or agents handles, collects, stores, disseminates or otherwise deals with State Data, the Contractor represents and warrants that it has implemented and it shall maintain during the term of this Contract the highest industry standard administrative, technical, and physical safeguards and controls consistent with NIST *Special Publication 800-53* (version 4 or higher) and *Federal Information Processing Standards Publication* 200 and designed to (i) ensure the security and confidentiality of State Data; (ii) protect against any anticipated security threats or hazards to the security or integrity of the State Data; and (iii) protect against unauthorized access to or use of State Data. Such measures shall include at a minimum: (1) access controls on information systems, including controls to authenticate and permit access to State Data only to authorized individuals and controls to prevent the Contractor employees from providing State Data to unauthorized individuals who may seek to obtain this information (whether through fraudulent means or otherwise); (2) industry-standard firewall protection; (3) encryption of electronic State Data while in transit from the Contractor networks to external networks; (4) measures to store in a secure fashion all State Data which shall include, but not be limited to, encryption at rest and multiple levels of authentication; (5) dual control procedures, segregation of duties, and pre-employment criminal background checks for employees with responsibilities for or access to State Data; (6) measures to ensure that the State Data shall not be altered or corrupted without the prior written consent of the State; (7) measures to protect against destruction, loss or damage of State Data due to potential environmental hazards, such as fire and water damage; (8) staff training to implement the information security measures; and (9) monitoring of the security of any portions of the Contractor systems that are used in the provision of the services against intrusion on a twenty-four (24) hour a day basis.

6.2 SECURITY BREACH NOTICE AND REPORTING

The Contractor shall have policies and procedures in place for the effective management of Security Breaches, as defined below, which shall be made available to the State upon request.

In the event of any actual security breach or reasonable belief of an actual security breach the Contractor either suffers or learns of that either compromises or could compromise State Data (a "Security Breach"), the Contractor shall notify the State within 24 hours of its discovery. Contractor shall immediately determine the nature and extent of the Security Breach, contain the incident by stopping the unauthorized practice, recover records, shut down the system that was breached, revoke access and/or correct

weaknesses in physical security. Contractor shall report to the State: (i) the nature of the Security Breach; (ii) the State Data used or disclosed; (iii) who made the unauthorized use or received the unauthorized disclosure; (iv) what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and (v) what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure. The Contractor shall provide such other information, including a written report, as reasonably requested by the State. Contractor shall analyze and document the incident and provide all notices required by applicable law.

In accordance with Section 9 V.S.A. §2435(b)(3), the Contractor shall notify the Office of the Attorney General, or, if applicable, Vermont Department of Financial Regulation ("DFR"), within fourteen (14) business days of the Contractor's discovery of the Security Breach. The notice shall provide a preliminary description of the breach. The foregoing notice requirement shall be included in the subcontracts of any of Contractor's subcontractors, affiliates or agents which may be "data collectors" hereunder.

The Contractor agrees to fully cooperate with the State and, to the extent the Security Breach is caused by Contractor's negligence or breach of its obligations under this Contract, assume responsibility at its own expense for the following, to be determined in the sole discretion of the State: (i) notice to affected consumers if the State determines it to be appropriate under the circumstances of any particular Security Breach, in a form recommended by the AGO; and (ii) investigation and remediation associated with a Security Breach, including but not limited to, outside investigation, forensics, counsel, crisis management and credit monitoring, in the sole determination of the State.

The Contractor agrees to comply with all applicable laws, as such laws may be amended from time to time (including, but not limited to, Chapter 62 of Title 9 of the Vermont Statutes and all applicable State and federal laws, rules or regulations) that require notification in the event of unauthorized release of personally-identifiable information or other event requiring notification.

In addition to any other indemnification obligations in this Contract, to the extent the Security Breach is caused by Contractor's negligence or breach of its obligations under this Contract, the Contractor shall fully indemnify and save harmless the State from any costs, loss or damage to the State resulting from a Security Breach or the unauthorized disclosure of State Data by the Contractor, its officers, agents, employees, and subcontractors.

6.3 SECURITY POLICIES

To the extent the Contractor or its subcontractors, affiliates or agents handles, collects, stores, disseminates or otherwise deals with State Data, the Contractor will have an information security policy that protects its systems and processes and media that may contain State Data from internal and external security threats and State Data from unauthorized disclosure, and will have provided a copy of such policy to the State. The Contractor shall provide the State with not less than thirty (30) days advance written notice of any material amendment or modification of such policies.

6.4 OPERATIONS SECURITY

To the extent the Contractor or its subcontractors, affiliates or agents handles, collects, stores, disseminates or otherwise deals with State Data, the Contractor shall cause an SSAE 18 SOC 2 Type 2 audit report to be conducted annually of its data centers housing State Data. The audit results and the Contractor's plan for addressing or resolution of the audit results shall be shared with the State within sixty (60) days of the Contractor's receipt of the audit results. Further, on an annual basis, within 120 days of the end of the Contractor's fiscal year, the Contractor shall transmit its annual audited financial statements to the State.

6.5 REDUNDANT BACK-UP

Onpoint shall maintain system redundancy and backups to achieve a 24-hour Recovery Point Objective and a 24-hour Recovery Time Objective.; The Contractor shall maintain fully redundant, client-facing systems, in multiple availability zones to achieve a 99.9 uptime. The Contractor's back-up policies shall be made available to the State upon request. The Contractor shall provide the State with not less than thirty (30) days advance written notice of any material amendment or modification of such policies.

6.6 VULNERABILITY TESTING

Onpoint shall run (or prove evidence of having been run) quarterly vulnerability assessments on externally facing assets storing or presenting state data including hosted or on premises infrastructure. Results will be delivered quarterly to the ADS security team, or technical lead for the program. Contractor shall remediate all critical/high issues within 90 days. Contractor shall provide a risk mitigation plan for medium and low issues. Contractor shall obtain written State approval for any exceptions. Contractor will work with the state to define a reporting process.

Onpoint will provide a copy of its HITRUST certification letter, HITRUST executive summary report, and annual penetration testing, annually, upon request.

7. CONTRACTOR'S REPRESENTATIONS AND WARRANTIES

7.1 GENERAL REPRESENTATIONS AND WARRANTIES

The Contractor represents, warrants and covenants that:

(i) The Contractor has all requisite power and authority to execute, deliver and perform its obligations under this Contract and the execution, delivery and performance of this Contract by the Contractor has been duly authorized by the Contractor.

(ii) There is no outstanding litigation, arbitrated matter or other dispute to which the Contractor is a party which, if decided unfavorably to the Contractor, would reasonably be expected to have a material adverse effect on the Contractor's ability to fulfill its obligations under this Contract.

(iii) The Contractor will comply with all laws applicable to its performance of the services and otherwise to the Contractor in connection with its obligations under this Contract.

(iv) The Contractor (a) owns, or has the right to use under valid and enforceable agreements, all intellectual property rights reasonably necessary for and related to delivery of the services and provision of the Deliverables as set forth in this Contract; (b) shall be responsible for and have full authority to license all proprietary and/or third party software modules, including algorithms and protocols, that Contractor incorporates into its product; and (c) none of the Deliverables or other materials or technology provided by the Contractor to the State will infringe upon or misappropriate the intellectual property rights of any third party.

(v) The Contractor has adequate resources to fulfill its obligations under this Contract.

(vi) Neither Contractor nor Contractor's subcontractors has past state or federal violations, convictions or suspensions relating to miscoding of employees in NCCI job codes for purposes of differentiating between independent contractors and employees.

7.2 CONTRACTOR'S PERFORMANCE WARRANTIES

Contractor represents and warrants to the State that:

(i) All Deliverables will be free from material errors and shall perform in accordance with the specifications therefor for a period of at least one year.

(ii) Contractor will provide to the State commercially reasonable continuous and uninterrupted access to the Service, and will not interfere with the State's access to and use of the Service during the term of this Contract;

(iii) The Service is compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its documentation;

(iv) Each and all of the services shall be performed in a timely, diligent, professional and skillful manner, in accordance with the highest professional or technical standards applicable to such services, by qualified persons with the technical skills, training and experience to perform such services in the planned environment.

(v) All Deliverables supplied by the Contractor to the State shall be transferred free and clear of any and all restrictions on the conditions of transfer, modification, licensing, sublicensing and free and clear of any and all liens, claims, mortgages, security interests, liabilities and encumbrances or any kind.

(vi) Any time software is delivered to the State, whether delivered via electronic media or the internet, no portion of such software or the media upon which it is stored or delivered will have any type of software routine or other element which is designed to facilitate unauthorized access to or intrusion upon; or unrequested disabling or erasure of; or unauthorized interference with the operation of any hardware, software, data or peripheral equipment of or utilized by the State. Without limiting the generality of the foregoing, if the State believes that harmful code may be present in any software delivered hereunder, Contractor will, upon State's request, provide a new or clean install of the software. Notwithstanding the foregoing, Contractor assumes no responsibility for the State's negligence or failure to protect data from viruses, or any unintended modification, destruction or disclosure.

(vii) To the extent Contractor resells commercial hardware or software it purchased from a third party, Contractor will, to the extent it is legally able to do so, pass through any such third party warranties to the State and will reasonably cooperate in enforcing them. Such warranty pass-through will not relieve the Contractor from Contractor's warranty obligations set forth herein.

7.3 LIMITATION ON DISCLAIMER

The express warranties set forth in this Contract shall be in lieu of all other warranties, express or implied.

7.4 EFFECT OF BREACH OF WARRANTY

If, at any time during the term of this Contract, software or the results of Contractor's work fail to perform according to any warranty of Contractor under this Contract, the State shall promptly notify Contractor in writing of such alleged nonconformance, and Contractor shall, at its own expense and without limiting any other rights or remedies of the State hereunder, re-perform or replace any services that the State has determined to be unsatisfactory in its reasonable discretion. Alternatively, with State consent, the Contractor may refund of all amounts paid by State for the nonconforming deliverable or service.

8. PROFESSIONAL LIABILITY AND CYBER LIABILITY INSURANCE COVERAGE

In addition to the insurance required in Attachment C to this Contract, before commencing work on this Contract and throughout the term of this Contract, Contractor agrees to procure and maintain (a)

Technology Professional Liability insurance for any and all services performed under this Contract, with minimum third party coverage of $1,000,000 per claim, $3,000,000 aggregate; and (b) first party Breach Notification Coverage of not less than $2,000,000.

Before commencing work on this Contract the Contractor must provide certificates of insurance to show that the foregoing minimum coverages are in effect.

With respect to the first party Breach Notification Coverage, Contractor shall name the State of Vermont and its officers and employees as additional insureds for liability arising out of this Contract.

9. LIMITATION OF LIABILITY

CONTRACTOR'S LIABILITY FOR DAMAGES TO THE STATE ARISING OUT OF THE SUBJECT MATTER OF THIS CONTRACT SHALL NOT EXCEED THREE TIMES THE MAXIMUM AMOUNT PAYABLE UNDER THIS CONTRACT. LIMITS OF LIABILITY FOR STATE CLAIMS SHALL NOT APPLY TO STATE CLAIMS ARISING OUT OF: (A) CONTRACTOR'S OBLIGATION TO INDEMNIFY THE STATE; (B) CONTRACTOR'S CONFIDENTIALITY OBLIGATIONS TO THE STATE; (C) PERSONAL INJURY OR DAMAGE TO REAL OR PERSONAL PROPERTY; (D) CONTRACTOR'S GROSS NEGLIGENCE, FRAUD OR INTENTIONAL MISCONDUCT; OR (E) VIOLATIONS OF THE STATE OF VERMONT FRAUDULENT CLAIMS ACT. IN NO EVENT SHALL THIS LIMIT OF LIABILITY BE CONSTRUED TO LIMIT CONTRACTOR'S LIABILITY FOR THIRD PARTY CLAIMS AGAINST THE CONTRACTOR WHICH MAY ARISE OUT OF CONTRACTOR'S ACTS OR OMISSIONS IN THE PERFORMANCE OF THIS CONTRACT. NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL OR SPECIAL DAMAGES, DAMAGES WHICH ARE UNFORESEEABLE TO THE PARTIES AT THE TIME OF CONTRACTING, DAMAGES WHICH ARE NOT PROXIMATELY CAUSED BY A PARTY, SUCH AS LOSS OF ANTICIPATED BUSINESS, OR LOST PROFITS, INCOME, GOODWILL, OR REVENUE IN CONNECTION WITH OR ARISING OUT OF THE SUBJECT MATTER OF THIS CONTRACT.

The provisions of this Section shall apply notwithstanding any other provisions of this Contract or any other agreement.

10. TRADE SECRET, PATENT AND COPYRIGHT INFRINGEMENT

The State shall not be deemed to waive any of its rights or remedies at law or in equity in the event of Contractor's trade secret, patent and/or copyright infringement.

11. REMEDIES FOR DEFAULT; NO WAIVER OF REMEDIES

In the event either party is in default under this Contract, the non-defaulting party may, at its option, pursue any or all of the remedies available to it under this Contract, including termination for cause, and at law or in equity.

No delay or failure to exercise any right, power or remedy accruing to either party upon breach or default by the other under this Contract shall impair any such right, power or remedy, or shall be construed as a waiver of any such right, power or remedy, nor shall any waiver of a single breach or default be deemed a waiver of any subsequent breach or default. All waivers must be in writing.

12. NO ASSUMPTION OF COSTS

Any requirement that the State defend or indemnify Contractor or otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or license verification costs of Contractor, is hereby deleted from the Contractor Documents.

13. TERMINATION

Upon termination of this Contract for any reason whatsoever, Contractor shall immediately deliver to the State all State information, State Intellectual Property or State Data (including without limitation any Deliverables for which State has made payment in whole or in part) ("State Materials"), that are in the possession or under the control of Contractor in whatever stage of development and form of recordation such State property is expressed or embodied at that time.

In the event the Contractor ceases conducting business in the normal course, becomes insolvent, makes a general assignment for the benefit of creditors, suffers or permits the appointment of a receiver for its business or assets or avails itself of or becomes subject to any proceeding under the Federal Bankruptcy Act or any statute of any state relating to insolvency or the protection of rights of creditors, the Contractor shall immediately return all State Materials to State control; including, but not limited to, making all necessary access to applicable remote systems available to the State for purposes of downloading all State Materials.

Contractor shall reasonably cooperate with other parties in connection with all services to be delivered under this Contract, including without limitation any successor provider to whom State Materials are to be transferred in connection with termination. Contractor shall assist the State in exporting and extracting the State Materials, in a format usable without the use of the Services and as agreed to by State, at no additional cost.

Any transition services requested by State involving additional knowledge transfer and support may be subject to a contract amendment for a fixed fee or at rates to be mutually agreed upon by the parties.

If the State determines in its sole discretion that a documented transition plan is necessary, then no later than sixty (60) days prior to termination, Contractor and the State shall mutually prepare a Transition Plan identifying transition services to be provided.

14. ACCESS TO STATE DATA

The State may import or export State Materials in part or in whole at its sole discretion at any time (24 hours a day, seven (7) days a week, 365 days a year), during the term of this Contract or for up to [three (3) months] after the Term (so long as the State Materials remain in the Contractor's possession) without interference from the Contractor in a format usable without the Service and in an agreed-upon file format and medium at no additional cost to the State.

The Contractor must allow the State access to information such as system logs and latency statistics that affect its State Materials and or processes.

The Contractor's policies regarding the retrieval of data upon the termination of services have been made available to the State upon execution of this Contract under separate cover. The Contractor shall provide the State with not less than thirty (30) days advance written notice of any material amendment or modification of such policies.

15. AUDIT RIGHTS

Contractor will maintain and cause its permitted contractors to maintain a complete audit trail of all transactions and activities, financial and non-financial, in connection with this Contract. Contractor will provide to the State, its internal or external auditors, clients, inspectors, regulators and other designated representatives, at reasonable times (and in the case of State or federal regulators, at any time required by such regulators) access to Contractor personnel and to any and all Contractor facilities or where the required information, data and records are maintained, for the purpose of performing audits and inspections (including unannounced and random audits) of Contractor and/or Contractor personnel and/or any or all of the records, data and information applicable to this Contract.

At a minimum, such audits, inspections and access shall be conducted to the extent permitted or required by any laws applicable to the State or Contractor (or such higher or more rigorous standards, if any, as State or Contractor applies to its own similar businesses, operations or activities), to (i) verify the accuracy of charges and invoices; (ii) verify the integrity of State Data and examine the systems that process, store, maintain, support and transmit that data; (iii) examine and verify Contractor's and/or its permitted contractors' operations and security procedures and controls; (iv) examine and verify Contractor's and/or its permitted contractors' disaster recovery planning and testing, business resumption and continuity planning and testing, contingency arrangements and insurance coverage; and (v) examine Contractor's and/or its permitted contractors' performance of the Services including audits of: (1) practices and procedures; (2) systems, communications and information technology; (3) general controls and physical and data/information security practices and procedures; (4) quality initiatives and quality assurance, (5) contingency and continuity planning, disaster recovery and back-up procedures for processes, resources and data; (6) Contractor's and/or its permitted contractors' efficiency and costs in performing Services; (7) compliance with the terms of this Contract and applicable laws, and (9) any other matters reasonably requested by the State. Contractor shall provide and cause its permitted contractors to provide full cooperation to such auditors, inspectors, regulators and representatives in connection with audit functions and with regard to examinations by regulatory authorities, including the installation and operation of audit software.

16. DESTRUCTION OF STATE DATA

At any time during the term of this Contract within (i) thirty days of the State's written request or (ii) [three (3) months] of termination or expiration of this Contract for any reason, and in any event after the State has had an opportunity to export and recover the State Materials, Contractor shall at its own expense securely destroy and erase from all systems it directly or indirectly uses or controls all tangible or intangible forms of the State Materials, in whole or in part, and all copies thereof except such records as are required by law. The destruction of State Data and State Intellectual Property shall be performed according to National Institute of Standards and Technology (NIST) approved methods. Contractor shall certify in writing to the State that such State Data has been disposed of securely. To the extent that any applicable law prevents Contractor from destroying or erasing State Materials as set forth herein, Contractor shall retain, in its then current state, all such State Materials then within its right of control or possession in accordance with the confidentiality, security and other requirements of this Contract, and perform its obligations under this section as soon as such law no longer prevents it from doing so.

Further, upon the relocation of State Data, Contractor shall securely dispose of such copies from the former data location and certify in writing to the State that such State Data has been disposed of securely. Contractor shall comply with all reasonable directions provided by the State with respect to the disposal of State Data.

17. CONTRACTOR BANKRUPTCY

Contractor acknowledges that if Contractor, as a debtor in possession, or a trustee in bankruptcy in a case under Section 365(n) of Title 11, United States Code (the "Bankruptcy Code"), rejects this Contract, the State may elect to retain its rights under this Contract as provided in Section 365(n) of the Bankruptcy Code. Upon written request of the State to Contractor or the Bankruptcy Trustee, Contractor or such Bankruptcy Trustee shall not interfere with the rights of the State as provided in this Contract, including the right to obtain the State Intellectual Property.

18. SOFTWARE LICENSEE COMPLIANCE REPORT

In lieu of any requirement that may be in a Contractor Document that the State provide the Contractor with access to its System for the purpose of determining State compliance with the terms of the Contractor Document, upon request and not more frequently than annually, the State will provide Contractor with a certified report concerning the State's use of any software licensed for State use pursuant this Contract. The parties agree that any non-compliance indicated by the report shall not constitute infringement of the licensor's intellectual property rights, and that settlement payment mutually agreeable to the parties shall be the exclusive remedy for any such non-compliance.

19. SOV CYBERSECURITY STANDARD 19-01

All products and service provided to or for the use of the State under this Contract shall be in compliance with State of Vermont Cybersecurity Standard 19-01, which Contractor acknowledges has been provided to it, and is available on-line at the following URL:
https://digitalservices.vermont.gov/cybersecurity/cybersecurity-standards-and-directives

ATTACHMENT E
MAINTENANCE AND SUPPORT/SERVCIE LEVEL TERMS

Planned SLAs are as follows:

1. At the start of the Maintenance & Support period, and lasting throughout the duration of the Agreement, the GMCB and Onpoint agree to the following Service Level Standards:

Service Level Standard	Fees at Risk
Processing Time: Once all payer files included in an extract cycle have achieved DQ/PASS status in Onpoint's system, Onpoint shall supply to the GMCB all standard extract tables within 30 days and all non-standard analytic tables (e.g., groupers, measures, attribution) within 45 days.	1% of monthly fees at risk for every calendar day past the 30 or 45-day deadline, up to a maximum 8% of fees for only the applicable month.
Enclave Availability: Onpoint shall make its Analytic Enclave environment available 24 hours per day, 7 days per week, with 99.9% uptime, excluding scheduled downtime with a minimum of 5 business days' notice.	0.25% of monthly fees at risk for each 1-hour outage, up to a maximum 2% of fees for only the applicable month.
Issue Resolution, Response Time, and Escalation Procedures: • **Priority 1:** Issue acknowledgement within 30 minutes with a support representative engaged within 1 hour. A Priority 1 Issue is defined as a major systematic issue or production-affecting issue, with one or multiple systems or users down or performance seriously degraded during business hours. There is no possible workaround. • **Priority 2:** Issue acknowledgement within 4 business hours with a support representative engaged within 8 business hours. A Priority 2 issue is defined as a localized/isolated issue, affecting service performance. User is still able to perform tasks or a workaround is available. • **All Other Issues and Work Request:** Request acknowledged within 1 business day and a timeline for completion provided within 2 business days. A work request is defined as anything that is not a Priority 1 or Priority 2 issue and is a request not requiring immediate attention. All other issues are defined as an issue with a non-critical function and is not a Priority 1 or Priority 2 issue. A workaround is available.	Each SLA violation will hold a penalty of 2% of the fees for the applicable month only, up to a maximum of an 8% penalty.
Disaster Recovery Time Objective and Recovery Point Objective: This pertains to client-facing systems, including SFTP, the Onpoint CDM portal, and the Analytic Enclave and are as follows. • **Recovery Time Objective (RTO):** 24 hours • **Recovery Point Objective (RPO**): 24 hours	Each SLA violation will hold a penalty of 5% of fees for the applicable month.

2. Onpoint is accountable for all technologies and services directly supported by Onpoint within its infrastructure beginning at the ingress/egress point of Onpoint's systems as well as for subcontracted technologies and services.

3. The GMCB must request any Service Credit due hereunder within thirty (30) days of the conclusion of the month in which it accrues. The GMCB waives any right to Service Credits not requested within this 30-day period. Service Credits shall be issued once validated by the GMCB and applied toward the invoice received by the GMCB no later than two months following the GMCB's Service Credit request. All performance calculations and applicable Service Credits are based on Onpoint records and data unless the GMCB can provide Onpoint with technical evidence to the contrary.

4. These SLAs provides the GMCB's sole and exclusive remedy for any service interruptions, deficiencies, or failures as set forth in this attachment.

5. The above SLAs, including any remedies hereunder, shall not apply with respect to any Excluded Events. "Excluded Event" means any event that adversely impacts the service that is caused by (a) the acts or omissions of the GMCB, its employees, contractors or agents; (b) the failure or malfunction of equipment, applications, or systems not owned or controlled by Onpoint; (c) Force Majeure events; (d) scheduled or unscheduled maintenance outside the Onpoint controlled infrastructure; (e) any suspension of service by Onpoint permitted under the Agreement; and/or (f) the unavailability of required GMCB personnel, including as a result of failure to provide Onpoint with accurate, current contact information. For clarification, Onpoint is assumed to have control over the equipment, applications, systems, and infrastructure of any subcontractor, consultant, or vendors that it can directly manage. Onpoint is assumed not to have control over the equipment, applications, systems, and infrastructure of large, utility-like vendors such as an internet or network provider or cloud hosting service.

6. The GMCB shall not be eligible to accrue any otherwise applicable credits: (a) during any period in which the GMCB is past due on any amounts owed in connection with the Service and/or (b) before the start of the first full calendar month following the first full production run. The GMCB may not carry over to subsequent months any credits subject to the limits or exclusions of these SLAs.

7. In no event shall the credits accrued in any single calendar year exceed, in the aggregate across all service levels and events, five percent (5%) of the annual invoice amounts for the affected services.

ATTACHMENT F
Delivery Expectation Document (DED) and Delivery Acceptance Form (DAF)

Deliverable Acceptance Form template

DELIVERABLE ACCEPTANCE CERTIFICATE			
Client Name:			
Project Name:			
Submitted for:	☐ Partial Completion ☐ Full Completion ☐ OTHER		
TO BE COMPLETED BY SUBMITTER			
Date Submitted:	/ /	**Submitted by:**	
Date Requested for Response:	/ /		
Submitter's email:		**Submitter's Phone #**	- -
Describe Milestones Achieved and Basis for Acceptance			
Defined Success Criteria:			
Signature		**Title**	
TO BE COMPLETED BY CLIENT			
Date Returned:	/ /		
Returned by:			
Reviewers email:	@ .	**Reviewer's Phone**	- -
Action Taken:	☐ **Accept** ☐ **Reject** ☐ **OTHER:**		
If rejected, please indicate reason:	☐ **Supporting documents are incomplete** ☐ Project Management Team disagrees with information provided ☐ More information is needed (see below) ☐ Other (see below)		
If rejected, other comments	Submitter will address the reason(s) for this rejection and resubmit this form within business days.		
Other Comments, if any:			
Documents attached if any:			
Other:			
Authorized Signature		**Title:**	
Authorized Signature		**Title:**	
DELIVERABLE ACCEPTANCE CERTIFICATE			
This is to certify Client's final approval of the above-described Milestone. Client has conducted all inspections, analysis, and testing necessary for it to make this final determination of acceptance. This Milestone has been completed in accord with all contractual requirements relating to the Milestone. As a result of this final acceptance of the Milestone, Client authorizes (VENDOR NAME) to issue an invoice for the dollar amount of this certificate as set forth above, which amount shall be paid by the State in accordance with the payment terms of the above-referenced Contract between the parties. The individual signing this Certificate of Final Acceptance on behalf of Client does so with full authority to bind Client.			

Deliverable Acceptance Form template

DELIVERABLE ACCEPTANCE CERTIFICATE			
Client Name:			
Project Name:			
Submitted for:	☐ Partial Completion ☐ Full Completion ☐ OTHER		
TO BE COMPLETED BY SUBMITTER			
Date Submitted:	/ /	**Submitted by:**	
Date Requested for Response:	/ /		
Submitter's email:		**Submitter's Phone #**	- -
Describe Milestones Achieved and Basis for Acceptance			
Defined Success Criteria:			
Signature		**Title**	
TO BE COMPLETED BY CLIENT			
Date Returned:	/ /		
Returned by:			
Reviewers email:	@ .	**Reviewer's Phone**	- -
Action Taken:	☐ **Accept** ☐ **Reject** ☐ **OTHER:**		
If rejected, please indicate reason:	☐ **Supporting documents are incomplete** ☐ Project Management Team disagrees with information provided ☐ More information is needed (see below) ☐ Other (see below)		
If rejected, other comments	Submitter will address the reason(s) for this rejection and resubmit this form within business days.		
Other Comments, if any:			
Documents attached if any:			
Other:			
Authorized Signature		**Title:**	
Authorized Signature		**Title:**	
DELIVERABLE ACCEPTANCE CERTIFICATE			
This is to certify Client's final approval of the above-described Milestone. Client has conducted all inspections, analysis, and testing necessary for it to make this final determination of acceptance. This Milestone has been completed in accord with all contractual requirements relating to the Milestone. As a result of this final acceptance of the Milestone, Client authorizes (VENDOR NAME) to issue an invoice for the dollar amount of this certificate as set forth above, which amount shall be paid by the State in accordance with the payment terms of the above-referenced Contract between the parties. The individual signing this Certificate of Final Acceptance on behalf of Client does so with full authority to bind Client.			