

Appendix M
SOW#4
To OFM RFP #15-1400

Statement of Work Number 4
to
Contract Number [XXX-XXX-XXX]
for
Washington All Payer Health Care Claims Database

This Statement of Work (SOW) is made and entered by and between the Office of Financial Management (“OFM”), and *[Legal Name of successful Bidder]* (“Lead Organization”), and is subject to the terms and conditions of Contract Number *[XXX-XXX-XXX]* in effect between the OFM and the Lead Organization.

OFM and Lead Organization agree as follows:

1. Project or Task Objectives

In performing the work and creating the deliverables hereunder, the Lead Organization is subject to requirements set forth in Chapter 246, Laws of 2015.

Services

1. Conduct maintenance and operations of the WA-APCD to ensure the functionality of the system over time.

Maintain security and privacy as required by the WA-APCD Law and the current OCIO Standard for Securing Information Technology Assets (current Standard Number 141.10 at: <https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>).

2. Perform Data Functions of the System

Collect data as required by the Data Submission Guide, OFM rule and the WA-APCD Law. At the direction of OFM, and to the extent necessary and as agreed, the Lead Organization shall work with the Data Vendor to:

- a. Collect, Transfer and, Stage Data. Including the design of data collection mechanisms with consideration for the time and cost incurred by data suppliers and others in submission and collection and the benefits that measurement would achieve, ensuring the data submitted meets quality standards and are reviewed for quality assurance.
- b. Use the secure Data Submission Process and Data Submission Guide to collect and transfer data.
- c. Cleanse and Perform Quality Assurance of Data. At a minimum:

- i. Review data submitters' files according to standards established by OFM
 - ii. Assess each record's alignment with established format, frequency, and consistency criteria
 - iii. Maintain responsibility for quality assurance, including, but not limited to:
 - 1) The accuracy and validity of data suppliers' data
 - 2) Accuracy of dates of service spans
 - 3) Maintaining consistency of record layout and counts
 - 4) Identifying duplicate records
 - 5) De-duplicate the data as necessary
 - vi. Demonstrate internal controls and affiliations with separate organizations as appropriate to ensure safe data collection, security of the data with state of the art encryption methods, actuarial support, and data review for accuracy and quality assurance
 - d. Identity Match, Longitudinalize and assign Unique Identifiers. At a minimum:
 - i. Perform identity matching on claims data with existing individuals in the WA-APCD
 - ii. Longitudinalize the data by matching individuals' claims over the time span of all data and across all payers
 - iii. assign unique identifiers as defined in RCW 43.371.010 as modified by Chapter 246, Laws of 2015, to individuals represented in the database.
 - e. Load and Store Data. At a minimum:
 - i. Store data on secure servers that are compliant with the federal Health Insurance Portability and Accountability Act (HIPAA) and regulations, with access to the data strictly controlled and limited to staff with appropriate training, clearance, and background checks
 - ii. Ensure that no claims data is purged from the system except as otherwise required by law or directed by OFM.
 - f. Maintain state of the art security standards for transferring data to approved data requestors
 - g. Ensure all patient-specific information is encrypted with an up-to-date industry standard encryption algorithm.
3. Update the Master Provider Roster and keep it current to within six months
4. Continue to request voluntary submission of claims data from self-insured organizations
5. WA-APCD Data Processes

The Lead Organization shall conduct the

- a. Data Access Governing Process
- b. Data Request Process
 - a. Where the lead organization acts in its capacity as a private entity, it may only access data pursuant to RCW 43.371.050 (4) (c) or (d).
- c. Establish Data Use Agreements with data recipients
- d. Data Release Process
- e. Comparison Report Verification Process

Update and maintain the above as required by law, rule or process.

- 6. Conduct WA-APCD Advisory Committees, as required
- 7. Perform education and outreach related to the WA-APCD and claims data for various audiences including, but not limited to the health care consumers, purchasers, providers and payers.
- 8. Perform fee-based activities to sustain the Lead Organization and WA-APCD
- 9. Update WA-APCD fees as necessary
 - a. Any fees must be approved by OFM
 - b. Any fees should be comparable, accounting for relevant differences across data requests and uses
 - c. The Lead Organization may not charge providers or data suppliers fees other than fees directly related to requested reports
 - d. Fees must be created and may only be changed using the process established in rule by OFM

- 10. Maintain the WA-APCD Website

The Lead Organization shall maintain and update the information produced under SOW#2 and published on the WA-APCD website. Such updates shall be in accordance with protocols and practices established in collaboration with OFM.

Report Deliverables

The Lead Organization shall produce the following Report Deliverables

- a. Annual Security Report for the Office of the Chief Information Officer (Chapter 246, Laws of 2015, Section 2 (4))

Due to the OCIO with a copy to OFM by September 1 of each year, starting September 1, 2017

- (a) Compliance with all applicable federal, state, and foreign privacy and data protection laws, as well as all other applicable regulations and directives in its collection, access, use, storage, disposal and disclosure of health care claims data.

- (b) Implementation of administrative, physical and technical safeguards to protect Personal Information that are no less rigorous than accepted industry practices including the International Organization for Standardization’s standards ISO-IEC 27002:2013 – Code of Practice for International Security Management, the Control Objectives for Information and related Technology (COBIT) standards and the State of Washington Office of the Chief Information Officer (OCIO) IT Security Policy and Standards.
 - (c) The manner in which Personal Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Agreement.
 - (d) Documentation of compliance with all applicable security polices and standards as required, including:
 - i. Documentation of organizational security program outlining its security policies and practices, which conform to those outlined and required in this agreement.
 - ii. Results of annual compliance audits including findings and mitigations, and expected compliance date
 - iii. Incident response plan including notification procedures to the Lead Agency and the State Office of Financial Management
 - iv. Documented communication plan regarding breach notification including notification to the State of Washington Chief Information Officer (CIO) and State Chief Information Security Officer (CISO).
 - v. Statement on Standards for Attestation Agreements (SSAE) No. 16 Service Organization Control 2 (SOC 2) Type II audit report.
 - (e) Adherence to OCIO standards—Implementation of administrative, physical and technical safeguards to protect Personal Information that are no less rigorous than the current OCIO Security Standards (OCIO 141.10) relating to Securing Information Technology Assets Standards.
- b. Annual List of Lead Organization Reports and Data Products for the Upcoming Year (Chapter 246, Laws of 2015, Section 6 (1) (b))

Due to the OFM Director by October 31st of each year, starting October 31, 2016

The lead organization shall submit to the director a list of Reports and Data Products it anticipates producing using WA-APCD data during the following calendar year.

For each report and data product to be produced, provide the following:

1. The stated purpose of the request
2. Explanation of how the request supports the goals of the WA-APCD
3. Description of the proposed methodology
4. Specific variables requested from the WA-APCD and an explanation of how the data is necessary to achieve the stated purpose described

In general, please provide:

1. How the Lead Organization will ensure all requested data is handled in accordance with the privacy and confidentiality protection required under the WA-APCD Law and any other applicable law
2. The method by which the data will be stored or destroyed
3. The protections that will be utilized to keep the data from being used for any purpose not authorized through this request
4. Consent to the penalties associated with the inappropriate disclosures or uses of direct patient identifiers, indirect patient identifiers, or proprietary information adopted under RCW 43.371.070 (1)

c. Annual Submission Compliance Status Report
(Chapter 246, Laws of 2015, Section 3 (3))

Due to the OFM by July 31 of each year, starting July 31, 2017

d. Lead Organization Annual Report

Due to OFM by August 31 of each year, starting August 31, 2016

This report shall include:

- i. Revenues
- ii. Expenditures
- iii. Outreach and Education Conducted
- iv. Details on the Data Requests Received, Approved and Denied
- v. Data Products Produced as the Lead Organization

e. Updated Sustainability Plan

Due to OFM by August 31 of each year, starting August 31, 2016

f. Ad-Hoc Reports

The Lead Organization may issue reports at the request of providers, facilities, employers, health plans and other entities

2. Timeline and Period of Performance

The period of performance for this project will start on October 1, 2016 and the work tasks are estimated to continue through the initial term of the Contract. Thereafter, OFM has the right to extend or terminate this SOW at its sole discretion.

No work shall be performed by Lead Organization until this SOW is executed by Lead Organization and OFM and is received by Lead Organization.