RFP 22-70302

Attachment K - Scope of Work

1. Background, General Requirements, and Key Definitions

1.1 Background

The purpose of the Indiana Department of Insurance (IDOI) is to protect Hoosiers as they purchase and use insurance products to keep their assets and their families from loss or harm. Consumers may need assistance with certain claim situations or just help in understanding how their policies work. The IDOI's other primary obligation is to monitor the financial solvency of the insurance companies domiciled in Indiana so that the legal promises made in insurance policies are honored.

During the 2020 legislative session, the Indiana General Assembly created the All Payer Claims Database ("APCD") in Title 27 (Indiana Code Sec. 27-1-44.5). Pursuant to Indiana Code Sec. 27-1-44.5-4, passed during the 2021 legislative session, the IDOI shall issue an RFP for an entity to create, operate and maintain the APCD.

The APCD will be a large-scale database that collects and aggregates significant amounts of data, including but not limited to, eligibility data, medical claims, pharmacy prescription drug claims, non-fee-for-service information, and health care provider data. The APCD's purpose is to facilitate the following:

1. Identifying health care needs and informing health care policy.
2. Comparing costs between various treatment settings and approaches.
3. Providing information to consumers and purchasers of health care.
4. Improving the quality and affordability of patient health care and health care coverage.

1.2 Key Definitions

Key definitions referenced in this attachment and Attachment F – Technical Proposal are defined below.

Document Terms	Definition
Administrator	Contractor; the entity the State enters into a contract with to provide the services described in the Contract
Advisory Board	See Indiana Code Section 27-1-44.5-0.4 for definition

Development	Creating / Coding a totally new application to meet defined agency / State requirements.
Customization	Adding or modifying code within an existing application to meet specific agency / State requirements.
Configuration	Modifying an application without adding / modifying code to meet specific agency requirements.
Executive Director	See Indiana Code Section 27-1-44.5-1.2 for definition
Health Payer	See Indiana Code Section 27-1-44.5-2 for definition
Hosting	Owning / Maintaining the Information Technology infrastructure required to house the application, database, and other technologies required by the application.
Project Management	Using specific knowledge, skills, tools, and techniques to deliver something of value to people.
Maintenance	Modifying an existing application via custom coding or configuration changes to correct issues or to enhance performance / usability to meet current and ongoing State requirements.
Testing	Confirming through a multi-phased process, that the solution delivered as part of the project meets the requirements and does so with the expected and acceptable level of quality.
Training	Delivering activities that enable users to effectively and efficiently leverage the solution in a manner needed for success.
Submitter	An entity that submits data to the APCD
Support	Providing help desk functions to application users via phone, e-mail, live support software, or a website and ensuring the application is available for use to meet state expectations.

Post Go-Live Support	Enhanced support for a short period of time directly after the project go-live to help expedite the stabilization of the solution (often called hyper-care).

1.3 Current Environment in Indiana

While there have been various efforts to aggregate health care data in the past, data aggregation in the magnitude and scale of the Indiana APCD provides an unprecedented opportunity for the State of Indiana. At this time, Indiana has the inter-agency and community support, funding, and leadership to standardize, collect, analyze, report, and benchmark data necessary to improve patient safety, reduce health care spending, and provide the quality and affordability of patient health care and health care coverage.

Many health plans, third party administrators, and pharmaceutical benefit managers do business in Indiana. The IDOI anticipates approximately 1,800,000 covered lives will be reported to the APCD by insurers writing individual and small group policies. In addition, the APCD will be receiving data from Medicaid and managed care entities. A self-insured employer may opt-in to share claims data with the database. The APCD may also obtain non-fee-for-service data and data from other sources, such as the Department of Health or hospitals. In total, data for approximately 5 million Hoosiers shall be hosted in the Administrator's data warehouse.

1.4 General Administrator Requirements

The IDOI intends to secure a Contract to obtain the services of an Administrator with expertise in the design, development, testing, project management, implementation, and operations of a large claims database. The Administrator sought should have experience in implementation, planning, design and analysis of databases and technical infrastructure that collect, create, and receive insurance and plan claims data and other non-fee-for-service information from all Submitters into a statewide information repository. The Administrator shall have the experience, capacity, and technical infrastructure necessary to collect and secure data from various Submitters, including a proven track record for performing consumer price transparency and other consumer-oriented information as a product. The Administrator shall have robust data encryption and member anonymization capability in accordance with the Health Insurance Portability and Accountability Act (42 U.S.C. 201 et seq.), as amended ("HIPAA").

2. Minimum Requirements

The Respondent and their proposed subcontractors must be able to meet the below Minimum Requirements. Failure to do so may be considered grounds for disqualification from further consideration per RFP Section 3.2, Step 1. The Respondent and their proposed subcontractors must state their ability and willingness to meet these Minimum Requirements in their Technical Proposal response. It is preferable that the Respondent meets these Minimum Requirements

independently, however Minimum Requirement adherence can be satisfied by a proposed subcontractor.

The Respondent must meet the following Minimum Requirements in order to respond to this RFP:

1. Respondent must have a minimum of five (5) years of company experience providing data collection, management, or reporting services using health care claims or encounters for a large data system.
2. Respondent must have a minimum of five (5) years of company experience providing analytic services to either an APCD or other large health care data collection and reporting system.
3. Respondent must have a minimum of five (5) years of experience in meeting the following mandates regarding data collection and storage:
    a. Health Insurance Portability and Accountability Act (HIPAA) (https://www.cdc.gov/phlp/publications/topic/hipaa.html); and
    b. Health Information Technology for Economic and Clinical Health Act (HITECH) (https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html)
4. Staff to be assigned to this project by Respondent must have a minimum of fifteen (15) total years of experience combined in data collection, data management, reporting services using health care claims, encounters for a large data system, or meeting HIPAA/HITECH mandates.
5. Respondent must currently be or agree to become a Center for Medicare and Medicaid Services (CMS) approved Custodian under a Data Use Agreement and Data Management Plan (for more information see: https://requests.resdac.org/request-material-tool). The Respondent must agree to be responsible for accepting, storing, and processing Medicare claims and eligibility data containing PHI. Respondent must agree to the non-negotiable terms and conditions required by CMS to act as a data custodian.
6. Respondent must currently be or agree to become CMS Qualified Entity (QE) (https://www.qemedicaredata.org/).
7. Respondent must furnish a copy of their most recent SOC 2 report.

3. High-Level Solution and Administrator Requirements

3.1 Administrator Duties and Responsibilities

At a high-level, the Administrator's duties will include the following:

1. Prioritizing security and protection of personal identifiable information ("PII") and protected health information ("PHI") data, considering the volume and the sensitivity of the data hosted within the APCD data warehouse;

2. Defining infrastructure needs and developing a sustainability plan;
3. Drafting a data submission guide
4. Collecting, managing, analyzing and hosting an online data submission portal or a proposed equivalent;
5. Collecting, storing, managing, and hosting all data collected by the APCD in an Administrator-developed centralized data warehouse or proposed equivalent;
6. Securing and streamlining data collection and aggregation;
7. Performing claims editing and business processing;
8. Performing data analytics and providing analytical tools and access to the end users;
9. Providing datasets and reports;
10. Furnishing data access for State-approved users;
11. Providing a consumer facing health care cost and quality decision support website and mobile application that are free to use and allow the public to view the average negotiated charges by each health carrier for specific health care services provided by an individual health care provider, as well as the quality metrics for facilities and health care providers for specific services;
12. Presenting data to allow for comparisons of geographic, demographic, and economic factors and institutional size;
13. Presenting data in a consumer-friendly manner in accordance with the Assistive Technology Policy (Section 508).

The Administrator, with input from the Executive Director and the Advisory Board:

1. Shall ensure the security of the data
2. Shall protect the privacy of the data in compliance with State of Indiana and federal law
3. Shall incorporate and utilize publicly available data other than administrative claims data if necessary to measure and analyze a significant health care quality, safety, or cost issue that cannot be adequately measured with administrative claims data alone
4. Shall ensure uniform data collection and determine the data elements to be collected, the reporting formats for data submitted, and the use and reporting of any data submitted, which shall align with national, regional, and other uniform all payer claims databases' standards where possible
5. Shall audit the accuracy of all data submitted and shall provide audit results in a report format agreed upon by the State of Indiana
6. Shall collect, aggregate, distribute, and publicly report performance data on cost, utilization, and pricing in a manner accessible for consumers, public and private purchasers, health care providers, and policymakers
7. Shall share data nationally or help develop a multistate effort if recommended by the Advisory Board
8. Shall share data for research and publication purposes if approved by the Advisory Board

The Executive Director will be dedicated to this project and will be able to support the Administrator throughout the duration of the Contract. IDOI subject matter experts may be made available to the Administrator on an as-needed basis.

4. Design, Development, and Implementation

The Administrator must design, develop, and implement an APCD that meets all expectations listed in the Scope of Work. The APCD will be used for the collection of health insurance information, potentially including claims for all Submitters, into a single statewide repository.

In order to design, develop, and implement the System, the Administrator should utilize a State-approved methodology. The Administrator shall propose a methodology (e.g., waterfall, agile) that best meets the needs and resource constraints of the State based on their experience with similar projects and environments.

The Administrator's System must have a network and database model (including an architectural diagram that outlines hardware/infrastructure required for the application to operate) that is approved by the State.

It is estimated that there will be roughly 8-10 internal users (with access to enter and process information) of the APCD. These internal users do not include individuals with access to the consumer website. However, regardless of the number of individuals accessing the consumer website or internal users, the APCD must be scalable with no impact to performance. Additionally, the Administrator must ensure the APCD has adequate storage technology and size to sustain all data. The data will be subject to data retention policies that will be developed at a later date.

The Administrator will begin by providing technical assistance and expertise to the IDOI during the planning process for development of the database. This will involve requirements gathering, which consists of defining, reviewing, confirming, validating, elaborating, and understanding the State's requirements, along with adding any other necessary solution requirements.

The Administrator shall then commence design planning and the development of design documents for the State's approval. The Administrator shall have established coding standards and methods that will be utilized during the design and development of the solution. The Administrator will then complete all necessary remaining steps to develop and deploy the database. The Administrator shall develop an implementation strategy and Test Plan (for more information, please see Section 8.1.2) that accounts for all key steps, considerations, and contingencies.

Successful system deployment will be accomplished when the Administrator completes the following activities:

- Provide access to nonproduction environments to the State team for implementation
- Inform IDOI of any technical preparation needed for implementation
- Develop all necessary Standard Operating Procedures and Checklists on state-approved templates

- Execute all State-approved activities in the Test Plan
- Conduct a walkthrough of implementation activities with the State team
- After the walkthrough, review the success of the walkthrough, objectives, lessons learned, user readiness, and operational readiness and determine whether to move forward with implementation
- Provide system support and address any issues needed throughout implementation
- Deliver a Formal System Acceptance Report
- Validate the system meets all security and technology requirements located https://www.in.gov/iot/policies-procedures-and-standards/
  Throughout design, development, and implementation, the Administrator must ensure the APCD prioritizes security and protection of personal identifiable information ("PII") and protected health information ("PHI") data (subject to HIPAA where applicable). The APCD must have a network and database model that aligns with the State's vision, as well as backup and recovery protocols and processes to protect all data. The Administrator must have a plan and strategy to manage unstructured data elements (e.g., emails, imaged documents, forms, reports, etc.).

The State would like Respondents to detail their proposed hosting approach in their Technical Proposal response, however, the State reserves the right to utilize one of the State's cloud tenants for hosting purposes.

5. Security and Privacy

5.1 Data Maintenance Services, Security, and Privacy

The Administrator shall employ security measures that ensure the APCD and the data collected by the APCD and information are protected. The Administrator shall ensure that the data collected by the APCD will only be used or included in book-of-business benchmarking data when combined with a significant amount of data from other sources to ensure confidentiality. The Administrator shall ensure that data collected by the APCD will never be released in any form to anyone without the State's written consent. The Administrator shall be solely liable for all costs associated with any breach of the data collected by the APCD that is housed at the Administrator's location(s) including but not limited to notification and any damages assessed by the courts.

The Administrator shall be 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 IDOI. The Administrator shall comply with the requirements of HIPAA when applicable to the collection, storage, and release of health care data and other information.

The Administrator must be compliant with all Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) requirements (https://hitrustalliance.net/product-tool/hitrust-csf/). The Administrator shall, by the Contract start date, be HITRUST CSF

Validated and have a HITRUST CSF Certification. The Administrator shall submit proof of this compliance at the start of the Contract and once per year throughout the duration of the Contract.

5.2 Data Security and Privacy

The Administrator shall implement infrastructure that allows for the secure submission and acceptance of all data to be submitted. The Administrator shall be able to provide services for the deidentification of direct identifiers, the collection, quality assurance, consolidation, secure storage, and access to health insurance claims data. The Administrator shall ensure that all data is stored within the continental United States. The Administrator shall provide services that:

1. Are robust, extensible, and forward looking in design;
2. Use modern technologies that can migrate to the technologies and data submission methods of tomorrow;
3. Have flexibility to handle future person and health care provider related linkage and shared services with other health data systems;
4. Are efficient and effective;
5. Provide quality, consistency, and accessibility of information;
6. Are protective of patient privacy;
7. Perform in a collaborative relationship with Submitters to maximize the quality, completeness, and timeliness of submissions.
8. Follow all applicable policies, procedures, and standards of the Indiana Office of Technology at https://www.in.gov/iot/policies-procedures-and-standards/

The Administrator must develop and deliver a data security and privacy plan no later than fifteen (15) business days after the Contract start date. The data security and privacy plan must describe the steps the Administrator will take to ensure data security and privacy throughout the duration of the Contract.

6. Data Services

6.1 Data Collection Services

The Administrator will coordinate with the data Submitters. The Administrator will develop a communication plan and materials to introduce the Submitters to the APCD and its requirements. The Administrator shall provide data management services and review submitted files to ensure consistency, timeliness, completeness, uniqueness, and validity/accuracy. In creating, operating, and implementing the APCD, the Administrator shall:

1. Interact on a continuing basis with Submitters, insurers, health maintenance organizations, third party administrators, pharmacy benefit managers, and other entities managing claims to detect and solve problems related to regulations and the claims submission process; this interaction may include email or phone communications, written materials, website development, FAQs, and annual meetings

2. Lead meetings with Submitters if deemed necessary by the IDOI
3. Manage registration and training of data Submitters
4. Ensure consistent de-identifications of certain personal identifiers at such time as State and federal laws and rules require de-identification
5. Collect and process data from Submitters. Related responsibilities include, but are not limited to:
    a. Creating one or more secure submission methods
    b. Ensuring the process is compatible with different operating systems
    c. Accepting or rejecting, ensuring compliance with reporting specifications, and giving feedback on required data submissions
    d. Identifying the need for, accepting, and processing corrected and resubmitted data
    e. Following up with Submitters on data issues and responding to questions and comments from Submitters
    f. Maintaining a system to allow test submissions from Submitters
    g. Developing and maintaining data element and Submitter-specific thresholds
6. Produce, and provide to Submitters, a data submission manual that would supplement any Administrative Rules, as needed, to ensure the correct submission of the data
    a. The data submission manual shall be approved by the IDOI and provided on an Administrator-hosted website
    b. The data submission manual will be updated and redistributed to reflect changes in statute, rules, or other changes to submission methods, as needed
7. Track and communicate to the IDOI overdue and otherwise noncompliant Submitters
8. Provide email and phone Help Desk business support for Submitters, the IDOI, and other State Agencies Monday through Friday, 8:00 am to 5:00 pm ET, to support the correct submission of the data to the Administrator. The Administrator shall respond to all emails and voicemail messages within one (1) business day.
9. Link health care providers and health plan members across Submitters
10. Capture non-claims-based payment information (e.g., capitated, advanced primary care, bundled, and pay-for-performance payments)

6.2 Data Validation Services

The usefulness of the APCD will be dependent on the quality of the data collected. The Administrator shall identify, adopt, and adhere to a data quality framework including data quality metrics, performance thresholds and processes for continuous data quality improvement within the solution. The Administrator shall define, measure and monitor data quality on a regular basis, assess root causes of poor data quality, recommend solutions to identified data quality concerns from root cause analyses, and implement recommended solutions to improve solution data quality. The Administrator will work continually with all submitters and resolve any data discrepancies or data file communication challenges.

In addition, the Administrator shall perform data validation and quality checks that address the following topics:

- Duplication
- Validity
- Thresholds/ distributions
- Comparison/Per Member Per Month (PMPM) consistency
- Adjustment claims
- Health care provider or member data discrepancies

The Administrator shall provide a report to the State that summarizes the data validation and quality checks.

6.3 Data Consolidation Services

Data consolidation is an integral component to the overall functionality of the APCD. The Administrator will also be responsible for providing the following data consolidation services:

1. Consolidate and enhance data for analytic use. Requests for data will most likely be filtered by the State, but the Administrator may be asked to provide input on a request.
2. Produce a Data Dictionary containing detailed specifications and documentation for the consolidated data sets, including description of files, tables, data elements, codes, and completeness of elements. This should be accessible on the consumer website and provide both current and historical content as appropriate.
    a. A separate Data Dictionary shall be included with data set extracts provided to researchers.
    b. Entity relationship diagrams shall also be included with the Data Dictionary.
    c. The Data Dictionary shall include version control information to allow for tracking of all changes made over time.
3. Store consolidated data in a format that is efficiently designed for querying. The Database shall be designed to allow for time-specific dimensions where the descriptive meanings of codes change over time. The data will be available for direct ad hoc query and extract by the IDOI and other State Agencies.
4. Execute and include in the consolidated data a process that assigns a common provider identifier across all instances of a single provider entity, regardless of insurer or practice affiliation, while also maintaining in the consolidated data the data as submitted.
5. Execute and include in the consolidated data a process that assigns a common provider (group) practice identifier across all instances of a single provider practice entity, regardless of Submitter.
6. Execute and include in the consolidated data a process that assigns a common person identifier across all instances of a single person, regardless of Submitter, business line or relationship to the subscriber.

7. If directed by the IDOI at the conclusion of the Contract, supply IDOI with copies of all consolidated and unconsolidated data from Submitters in a comprehensive and organized manner including written documentation of the contents of the data files. End of Contract data shall be supplied in a format agreed to by the IDOI and the Administrator.
8. Amend the collection and consolidation system to keep current with any changes made to the statute or rules and any changes made to industry standard coding systems for the life of the Contract, including updates to the APCD-Common Data Layout (CDL) (if adopted) or the adoption of National Council for Prescription Drug Programs (NCPDP) and Accredited Standards Committee (ASC) X12N standards, at no additional cost to the State

7. Data Production and Consumer Website

In addition to data consolidation and data collection, data production is an essential component to achieving the purpose of the APCD as outlined in the Indiana Code. The Administrator will be responsible for the following data production services:

1. Create and maintain a consumer website where consumers can find price and quality information. The consumer website's design and layout are subject to State-approval.
2. Provide data sets on a quarterly and ad hoc basis to the IDOI in agreed upon format, including replacements of any prior time periods for data that has changed without additional cost to the IDOI
3. Upon request in writing, supply files covering custom periods and contents to the IDOI or other State Agencies
4. Provide releasable custom data sets to researchers and other parties, within ten (10) business days (or within a longer timeframe requested by the Administrator and approved by the State), as approved by the IDOI
5. Provide public use data sets, within five (5) business days of receipt of a proper request (or within a longer timeframe requested by the Administrator and approved by the State)
6. Maintain public-facing records of all releasable data requests on website
7. Produce, maintain, and publish on website complete documentation of the data sets including logic used to transform data and create derived data elements
8. Be responsible for notifying all data recipients of any extract, created for either public use or research purposes that was later identified to have issues, either due to Administrator or Submitter error, that significantly affects its usefulness and/or completeness, regardless of the cause of the issues. The notice shall include a description of the issues and their potential impact and an offer to send replacement data. The Administrator shall provide notices to the IDOI before release for review and approval.

8. Project Management

8.1 Project Management Plan and Project Schedule

Through project planning efforts, the Administrator shall develop a Project Management Plan (PMP) and Project Schedule. The PMP documents the actions necessary to define, prepare, integrate, and coordinate all subsidiary plans. It will define how the project will be executed, monitored, controlled, and closed, as well as the proposed methods and protocol for all features, functions, and milestone deadlines. The Administrator must deliver the PMP and the corresponding subsidiary plans within the first thirty (30) calendar days of the project. Subsidiary plans must be integrated into the PMP and are set forth in the subsections below. All plans are subject to State review, edits, and approval.

- Communication Management Plan
- Organizational Change Management (OCM) Plan
- Schedule Management Plan
- Resource Management Plan
- Scope Change Management Plan
- Configuration Management Plan
- Issue Management Plan
- Risk Management Plan
- Quality Management Plan

The Project Schedule must contain a detailed set of tasks/deliverables required and associated estimated timeframes to complete all activities required under this Scope of Work. It shall also contain a detailed description of the tasks, deliverables, critical events, task dependencies, Administrator and State Resources required, levels of effort, and risk for each task and deliverable.

The Project Management Plan, subsidiary plans, and the Project Schedule shall be updated monthly, unless otherwise approved by the State.

Furthermore, the Administrator shall complete the following Project Management requirements:

- Shall, on at least a bi-weekly basis, hold teleconferences at the Administrator's expense with IDOI staff and other parties invited by the IDOI to discuss project progress, concerns, and next steps (as project needs change, and upon agreement of the IDOI, the frequency of meetings may be reduced or increased).
- Shall provide written progress/status reports, to be submitted to the State every two (2) weeks. The reports should be keyed to the implementation portion of the Project Management Plan, subsidiary plans (if applicable), and the Project Schedule and include, at a minimum, an assessment of progress made, difficulties encountered, recommendations for addressing the problems, and changes needed to the Project Management Plan, subsidiary plans, or the Project Schedule.

- Shall provide a report of the status of progress, to be submitted to the State every two (2) weeks. This report shall be tied to the performance section of the Project Management Plan and/or a subsidiary plan and contain at least the following information:
    - A narrative review of progress made during the reporting period. This shall include the status of relationships with Submitters for the receipt of data and a summary of new/updated data received, as well as an outline of problems encountered and whether and how they were solved, and deliverables scheduled and delivered.
    - A summary of the problems that the Administrator encountered or might reasonably expect to encounter, and recommended solutions.
    - For services required but not rendered, or actions described in the Project Management Plan, a subsidiary plan, or the Project Schedule but not taken or completed, there shall be an explanation of the failure to meet the schedule and detailed plans to overcome the failure as well as to prevent its recurrence.
    - An update of the Project Management Plan and Project Schedule showing work completed, impact of schedules missed, and, if needed, desired changes to the Project Management Plan, a subsidiary plan, or the Project Schedule for the balance of the project. All changes to the Project Management Plan, a subsidiary plan, or the Project Schedule are subject to the prior approval of IDOI.

It is the State's expectation that the APCD will be have some functionality operable in 2023.

8.2 Test Plan

The Administrator shall also provide a Test Plan for IDOI approval. The Test Plan will include, at a minimum, identification, preparation, and Documentation of planned testing; a requirements traceability matrix; test variants; test scenarios; test cases; test scripts; test Data; test phases; unit tests; expected results; and a tracking method for reporting actual versus expected results as well as reporting for all errors and problems identified during test execution.

The IDOI will be presented with a Test Plan no less than thirty (30) business days after the start of the Contract. Test scenarios, test cases, test scripts, test data, and expected results, as well as written Certification of the Administrator's completion of the prerequisite tests, shall all be provided prior to IDOI staff involvement in any User Acceptance Testing ("UAT").

The Administrator shall complete the following requirements in developing and completing the Test Plan:

- The Administrator shall certify in writing, that the Administrator's own staff has successfully executed all prerequisite Administrator testing, along with reporting the actual testing results prior to the start of any testing executed by IDOI staff.
- The IDOI will be presented with an IDOI approved Final Test Plan, test scenarios, test cases, test scripts, test data, and expected results, as well as written Certification of the

Administrator's completion of the prerequisite tests, prior to IDOI staff involvement in any User Acceptance Testing ("UAT")

- The Administrator shall perform a performance and stress test by simulating an agreed-upon number of transactions by an agreed-upon number of users simultaneously or over a window of time to ensure the solution meets performance expectations.
- The Administrator, with IDOI, shall perform UAT that covers any aspect of the System, including administrative procedures such as backup and recovery. The results of the UAT provide evidence that the System meets the User Acceptance criteria as defined in the Test Plan.
- Upon successful conclusion of UAT and successful System deployment, the IDOI will confirm Acceptance.

8.3 Training Plan

The training effort is a vital piece to the successful implementation and acceptance of the new solution. The Administrator shall provide a high-quality training experience for internal users. The Administrator must develop and maintain a detailed Training Plan that outlines the training schedule and overall training strategy/plan for State users prior to and during implementation. The Training Plan must also include: key objectives, training tools, roles and responsibilities, training environments, approach and methodology, training types, and materials. The Administrator must provide a sufficient number of staff to successfully accomplish all of the requirements of the Training Plan. The Administrator's training group must have proven experience in the development and delivery of comprehensive training to support organizational transformation as it relates to a transition to a new system. The training group must have robust experience training end users and rolling out new systems.

The Administrator must ensure that training includes both new and refresher application user training. The new application user training must be relevant for new users that are trained during the Maintenance & Operations period. The training shall be updated after each post-implementation release, unless otherwise determined by the State. The training must include some form of online help system if required by State users (for more information, please see Section 9.1 4 Help Desk Services).

The Administrator must develop and maintain a repository for training materials that can be accessed by State users throughout the duration of the Contract.

8.4 Reporting and Transition Plan

The Administrator shall provide an annual report by July 1 of each year that provides, at a minimum, a detailed review of the operations under the Contract, including a discussion of problems encountered and resolved or outstanding and recommendations for change. Furthermore, the Administrator shall complete the following requirements in developing and completing its reports and transition plan:

- Shall, upon request, provide detailed documentation for all aspects of the project to ensure complete transparency of the processes used for collection, quality assurance testing, consolidation, and release of the data, including results of Administrator's testing of their solution.
- Shall turn over, at the conclusion of the Contract or if otherwise required due to early termination of the Contract, all data provided by Submitters to IDOI and electronic versions of all final application source code and documentation developed for the project, as well as full access to and control of the consumer website. This information should be provided in a format mutually agreed upon by IDOI and the Administrator.
- Shall, six (6) months prior to the conclusion of the Contract, develop a transition plan that upon expiration of the Contract shall assist IDOI in continuing collection of the data. The Administrator shall cooperate with any new Administrator or with IDOI staff to ensure all existing data is supplied and any code and documentation needed to provide continuity of the project is supplied to staff of the new Administrator and de-identification and consolidation methods are fully transferred. The plan shall include, but not be limited to:
    - Proposed approach for turnover
    - Tasks and subtasks for turnover
    - Schedule for turnover
    - Documentation updates for turnover

9. Maintenance, Support, and Enhancements

9.1 Maintenance & Support

After implementation, the Administrator shall begin providing system maintenance services to support the processes of the system's infrastructure and ensure availability to stakeholders. The Administrator shall manage and complete system maintenance activities associated with the solution starting at the full implementation of the solution until the Contract's base period end date. This work shall not include the responsibilities of the Administrator related to the warranty period (i.e., defect resolution shall be covered by the warranty period).

The Administrator shall, at a minimum, provide the following system maintenance services:

1. **System Maintenance.** The Administrator must plan and execute tasks required to ensure that all solution components stay relevant and useable. This support includes resolution of technical issues, application of patches, preventative maintenance, planning/execution of upgrades, and regular performance monitoring and performance reporting.
2. **System Performance Monitoring and Reporting.** The Administrator must utilize an issue tracking and management system to monitor and troubleshoot all solution components. The Administrator shall work with the State to plan and communicate scheduled maintenance or emergency maintenance as soon as the Administrator knows that maintenance will be needed. The Administrator shall submit system performance and

monitoring reports, regular submission reports, and real-time data submission status reports, in accordance with State requests.

3. **Incident Management.** The Administrator shall work with the State to generate an agreed upon incident and disaster response plan that explicitly defines roles/responsibilities and actions to be taken to respond to incidents and disasters. The Administrator shall properly plan and conduct services to minimize the occurrence of incidents and/or problems with the solution components and service delivery. If incidents and/or problems arise, the Administrator shall work with the State to resolve issues in a timely manner based on the severity/priority levels determined by the State. Additionally, the Administrator shall have a formal Disaster Recovery Plan that describes all disaster recovery activities and contingencies.
4. **Help Desk Services.** System users (including State staff, third party State Administrators, and all other potential users) shall have access to a technical help desk that provides answers to solution questions and addresses solution issues that arise. The Help Desk will route policy or training questions and issues to correct Administrator. The Administrator shall lead and staff the Help Desk team and include embedded staff from the State, if requested.

9.2 Post-Implementation Releases

For all releases after the solution has been implemented, the Administrator shall develop and execute Release Plans and distribute release notes describing specific changes that are part of the release. The Release Plan shall include but not be limited to, the following processes and activities:

a. Establishment and implementation of plans and procedures for the Release Management function
b. Rollout Planning – Plan for and schedule rollout of new services or sites
c. Release Planning – Plan for, coordinate, and schedule releases of new versions of the software, data, procedures, and training
d. Rollout Management – Deliver services to new sites or existing sites
e. Release Control – Monitor the release process and adhere to release schedules
f. Migration Control – Coordinate the promotion of new releases from development to test to production
g. Release Testing – Coordinate the actual testing of releases/updates. This includes specific tests for the new functionality and a set of regression tests that confirms key functionality that was already in place will continue to function as expected and is not negatively affected by the current release.
h. Software and Data Distribution – Verify delivery of the correct versions of the software, data, or configuration releases to all locations, regardless of hardware type (server, workstation, laptop, etc.)
i. Training – Train relevant stakeholders on the new processes and functions associated with the release

9.3 Enhancements

The Administrator shall provide a capped Enhancements Pool of 10,000 hours a year. These Enhancement Pool hours include project management, requirements gathering and validation, design, development, testing, and implementation needed for enhancements. The State is not required to use up the hours and dollars allocated for the Enhancements Pool for each year. Enhancements can be for new System components or modifications/configuration changes to existing System components. Any System improvement, adaptation, or other update that requires less than or equal to 60 hours of work shall be considered part of system maintenance services. The Administrator may propose enhancements during the contract; however, these hours may only be utilized with State pre-approval and sign off.

To utilize Enhancements, the Administrator and the State will follow an agreed-upon change request process. As part of this process, the Administrator will submit documentation with, for each Enhancement, the types of resources needed, associated levels of effort (for the State and the Administrator), timelines for implementation, cost, and risk that is incurred to implement the Enhancement. If the Enhancement requires updates to documentation, testing, and training, time and cost estimates must be provided for those updates.

The Administrator shall conduct comprehensive testing on all System components impacted by the Enhancement to find and resolve any defects. In addition, the Administrator must update existing test cases/scripts and create new test cases/scripts as needed for new functionality. The Administrator must update documentation including but not limited to training materials, design documentation, data dictionaries, that are affected by each release. Changes that are needed to fix an Enhancement after it is implemented and that are brought to the Administrator during the warranty period shall not count towards the Enhancements Pool.

9.4 Warranty

The Administrator will warranty the solution against any defects for a period of 90 days after implementation. Defects are errors or issues found after UAT that are rooted to an original requirement of the system. Defects can range from system failure (where no further processing is possible) to minor cosmetic changes (e.g., usability errors). All defects that are identified after UAT shall be covered by the warranty period.

Determination of defects after implementation will be reviewed by the State. Review will consist of analyzing the system issue with tools to determine if the cause is a true defect. Any resulting work effort to fix a defect or make changes to the system will follow State-approved processes. The State has a 90-day window (from each Go-Live) to identify defects, however, the warranty period will be extended until the defect and any connected defects are remedied.

10. Analytics

The Administrator is responsible for collaborating with the IDOI to develop an Analytics Plan that will aid in the development of an Analytic environment that is optimized for ease of use by APCD users with varying needs and skill sets. The State's system solution must provide flexibility and customization to extract, transform, and load data from hospitals and other entities, including producing regular reports to State agencies and interactive dashboards.

At a minimum, the Analytics Plan shall:

a. Describe how data produced by the Respondent will be accessed, extracted, or transferred into the analytic environment including expected timelines based on complexity of activity
b. Outline data quality control processes for specific use-cases identified in consultation with IDOI
c. Describe how hosting needs will be addressed
d. Address user access controls
e. Describe how data extracts or data marts can be developed to assist with identified analytic goals
f. Identify specific standard analytic reports that will be generated by the Respondent and the corresponding frequency
g. Include documentation and training for data users in the analytic environment
h. Define strategies for data back-up, disaster recovery (including system failure response/ recovery times), and secure data disposal.

At minimum the Analytics Plan's required functions include:

a. Regular data refresh (e.g., every 30 days)
b. Point-in-time reporting capabilities
c. Data review in the Analytic Environment prior to the data being made available to internal and external stakeholders
d. Producing a set of standard data sets with documentation that can be released to qualified users for qualified purposes. For each standard data set, the Respondent will produce meta-data and a data dictionary that documents applied edits and summary statistics. This will include both Limited Data Sets and Research Data Sets.

11. Billing & Invoicing, Corrective Action, and Payment Withholds

11.1 Billing & Invoicing

The State will reimburse the Administrator on a monthly basis for a flat fee for the duties and responsibilities outlined in the Scope of Work, excluding enhancements and warranty-related activities. Enhancement pricing will either follow the fixed fee deliverables-based approach or the time and materials-based approach based on Contractual hourly rates and change request process agreed to by the Administrator and the State. The State will determine the method to use for each enhancement. If services are provided in exchange for fixed or not-to-exceed

compensation, the Administrator is solely responsible for any costs in excess of the specified compensation. Changes covered by the Warranty will be provided to the State at no cost.

11.2 Corrective Action

It is the State's primary goal to ensure that the Administrator is accountable for delivering quality services as defined and agreed to in the Contract. This includes, but is not limited to, performing all items described in the Scope of Work, completing all deliverables in a timely manner, and generally performing to the satisfaction of the State. Failure to perform in a satisfactory manner may result in Corrective Actions and Payment Withholds described below.

The State may require corrective action(s) when the Administrator has failed to provide the requested services. The nature of the corrective action(s) will depend upon the nature, severity and duration of the deficiency and repeated nature of the non-compliance. Severity shall be determined by the State, in its sole discretion. The written notice of corrective actions may be instituted in any sequence and include, but are not limited to, any of the following:

- Written Warning: The State may issue a written warning and solicit a response regarding the Administrator's corrective action.

- Formal Corrective Action Plan: The State may require the Administrator to develop a formal corrective action plan to remedy the breach. The Corrective Action Plan must be approved by the State. If the Corrective Action Plan is not acceptable, the State may provide suggestions and direction to bring the Administrator into compliance.

If written warning is issued, the Administrator shall provide a written response regarding their proposed remedies within five (5) business days of the occurrence or State request.

If a formal Corrective Action Plan is requested, the Administrator shall submit, within ten (10) business days of the occurrence or State request a formal Corrective Action Plan (CAP) that addresses the causes of the deficiency, the impacts and the measures being taken and/or recommended to remedy the deficiency, and whether the solution is permanent or temporary. It shall also include a schedule showing when the deficiency shall be remedied, and for when the permanent solution shall be implemented, if appropriate. Upon State's approval of the CAP, the Administrator shall execute the CAP. The Administrator shall complete all necessary corrective measures within ninety (90) calendar days of discovery of an issue prompting a Corrective Action Plan unless an alternative schedule is agreed to by the State.

The Administrator shall provide updates on CAP progress to the State in an agreed upon cadences until the CAP has been successfully completed.

The Administrator shall seek the State's written release from the obligations of the CAP upon successful completion of the CAP and correction of performance.

11.3 Payment Withholds

Beginning the month in which a formal CAP is required per the Corrective Action paragraph above, the State may withhold up to 10% of total monthly fixed fee components of the invoice and all subsequent billing until the CAP is completed and the proposed remedy is implemented. When the CAP is completed, and the proposed remedy is implemented, all monies withheld shall be returned to the Administrator within thirty (30) days. Should the CAP not be submitted as required, or should the remedy not be implemented within the timeframe specified by the CAP, the withheld monies may be forfeited.